Fundusze Europejskie Infrastruktura i Środowisko | Rzeczpospolita Polska | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

DOSTAWA SYSTEMU BEZPIECZEŃSTWA (UTM), CENTRALNEGO SYSTEMU LOGOWANIA, SYSTEMU CENTRALNEGO ZARZĄDZANIA URZĄDZENIAMI BEZPIECZEŃSTWA WRAZ ZE SZKOLENIAMI

ZAMAWIAJĄCY:
POWIATOWA STACJA SANITARNO-EPIDEMIOLOGICZNA W SZCZECINKU
UL. ORDONA 22, 78-400 SZCZECINEK
e-mail: psse.szczecinek@sanepid.gov.pl
tel. (094} 374-05-59

Zaprasza do złożenia oferty w trybie art. 275 pkt 1 (w trybie podstawowym bez negocjacji) o wartości zamówienia nieprzekraczającej progów unijnych o jakich stanowi art. 3 ustawy z 11 września 2019 r. - Prawo zamówień publicznych (tj. Dz. U. z 2023 r. poz. 1605 ze zm.) - dalej ustawa PZP.

Nr postępowania: **PPIS.272.1.2023**

Załączniki:
1. Załącznik nr 1_formularz ofertowy
2. Załącznik nr 2_oświadczenie o braku podstaw wykluczenia wykonawcy
3. Załącznik nr 3_oświadczenie o spełnieniu warunków udziału w postępowaniu
4. Załącznik nr 4_oświadczenie wykonawców wspólnie ubiegających się o zamówienie
5. Załącznik nr 5_zobowiązanie
6. Załącznik nr 6_opis przedmiotu zamówienia – wykaz oferowanego sprzętu
7. Załącznik nr 7_ wzór umowy

ROZDZIAŁ I Podstawowe informacje o postępowaniu, tryb udzielania zamówienia

1. Zamawiający:
   - POWIATOWA STACJA SANITARNO-EPIDEMIOLOGICZNA W SZCZECINKU, Ul. ORDONA 22, 78-400 SZCZECINEK, NIP: 673-11-37-277, REGON: 330927448
   - numer telefonu: **(094) 374-05-59**
   - adres poczty elektronicznej: **psse.szczecinek@sanepid.gov.pl**
   - adres strony internetowej prowadzonego postępowania (na stronie tej udostępniane będą też zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia): **https://platformazakupowa.pl/pn/psse-szczecinek**
   - osobą uprawnioną do komunikowania się z wykonawcami jest Anna Woźniak tel.: (094) 374-05-59 w godz. 08:00-14:30,
   - godziny pracy zamawiającego: 07:25-15:00.
2. Nazwa postępowania: ,,Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, systemu centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami".
3. Podstawa prawna: ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2023r., poz.1605 ze zm.), zwana dalej ustawą Pzp.
4. Postępowanie jest prowadzone w trybie podstawowym bez negocjacji, na podstawie art. 275 pkt 1 ustawy.
5. Do udzielenia przedmiotowego zamówienia publicznego stosuje się przepisy dotyczące dostaw.
6. Do czynności podejmowanych przez zamawiającego i wykonawców w postępowaniu o udzielenie zamówienia publicznego stosuje się przepisy ustawy oraz aktów wykonawczych wydanych na jej podstawie, dotyczące zamówień o wartości równej lub przekraczającej kwotę 130 000 zł.
7. Do spraw nieuregulowanych w SWZ zastosowanie mają przepisy ustawy Pzp. Do spraw nieuregulowanych ustawą mają zastosowanie przepisy Kodeksu Cywilnego.
8. Zamówienie jest finansowane z w ramach realizacji projektu nr POIS.II.03.00-00-0192/22 pn. „Wzmocnienie infrastruktury powiatowych stacji sanitarno-epidemiologicznych w celu zwiększenia efektywności ich działania" realizowanego w ramach osi priorytetowej XI REACT-EU działania 11.3 Wspieranie naprawy i odporności systemu ochrony zdrowia Programu Operacyjnego Infrastruktura i Środowisko na lata 2014-2020 w zakresie wsparcia organów Państwowej Inspekcji Sanitarnej.
9. Zamawiający przewiduje możliwość unieważnienia postępowania o udzielenie zamówienia na podstawie art. 310 pkt. 1 ustawy Pzp jeżeli środki publiczne, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostaną mu przyznane.
10. Zamawiający nie dopuszcza składania ofert wariantowych.
11. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

ROZDZIAŁ II Informacje o środkach komunikacji elektronicznej. Wymagania techniczne i organizacyjne sporządzania, wysyłania i odbierania korespondencji elektronicznej

1. Informacje o środkach komunikacji elektronicznej, przy użyciu których zamawiający będzie komunikował się z wykonawcami:

1) Z zastrzeżeniem art. 61 ust. 2 ustawy, komunikacja między zamawiającym a wykonawcami, w tym oferty oraz wszelkie oświadczenia (w tym o wyjaśnienie treści SWZ), zawiadomienia i informacje przekazywane są wyłącznie poprzez ich złożenie na elektronicznej platformie „Open Nexus" pod adresem **https://platformazakupowa.pl** (zwana dalej „Platformą") i pod nazwą postępowania wskazaną w tytule SWZ.

2) Korespondencja przekazana zamawiającemu w inny sposób (np. listownie, mailem) nie będzie brana pod uwagę, z zastrzeżeniem pkt. 3.

3) W sytuacji awarii platformy „Open Nexus" lub przerwy technicznej jej działania Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres:

psse.szczecinek@sanepid.gov.pl *(nie dotyczy składania ofert).*

2. Wymagania techniczne i organizacyjne sporządzania, wysyłania i odbierania korespondencji elektronicznej.

1) **Ofertę i oświadczenie, o którym mowa w art. 125 ust. 1 ustawy, składa się, pod rygorem nieważnosc1 w formie elektronicznej (tj. przy użyciu kwalifikowanego podpisu elektronicznego) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
2) Sposób sporządzenia podmiotowych środków dowodowych, przedmiotowych 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.
3) W zależności od formatu podpisu (PAdES, XAdES) i jego typu (zewnętrzny, wewnętrzny) wykonawca dołącza do Platformy uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny):
   a) dokumenty w formacie „pdf" zaleca się podpisywać formatem PAdES,
   b) zamawiający dopuszcza podpisanie dokumentów w formacie innym niż „pdf", wtedy należy użyć formatu XAdES.
   Uwaga: W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dofqczenia odpowiedniej liczby plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES
4) Szczegółowe informacje o sposobie pozyskania:
   a) 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,
   b) profilu zaufanego można znaleźć pod adresem internetowym: https://www.gov.pl/web/gov/zaloz-profil-zaufany,
   c) podpisu osobistego można znaleźć pod adresem internetowym: https://www.gov.pl/web/e-dowod/podpis-osobisty.
5) Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
6) Zamawiający zaleca, aby wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
7) Formaty plików wykorzystywanych przez wykonawców powinny być zgodne z Obwieszczeniem Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".

Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) **ze szczególnym wskazaniem na .pdf.** W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów: **.zip, .72.**

8) Wymagania sprzętowe dla wykonawcy:
   a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych – MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   c) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
   d) włączona obsługa JavaScript,
   e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   f) Szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
   g) Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
9) W celu złożenia oferty wykonawca zobowiązany jest zapoznać się z Regulaminem Internetowej Platformy zakupowej platformazakupowa.pl Open Nexus Sp. z o.o. dostępnym na stronie Platformy pod adresem https://platformazakupowa.pl/strona/1-regulamin postępować zgodnie z instrukcją zawartą w nim.
10) Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
11) Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu składania ofert wycofać ofertę. Sposób dokonywania wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
12) Wykonawca nie może wycofać oferty po upływie terminu składania ofert.
13) Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie ani logowania do Platformy.
14) Komunikacja poprzez Wyślij wiadomość umożliwia dodanie do treści wysyłanej wiadomości plików lub spakowanego katalogu (załączników). Występuje limit objętości plików lub spakowanych folderów do ilości 10 plików lub spakowanych folderów przy maksymalnej sumarycznej wielkości 500 MB.
15) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
16) Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
17) Występuje limit objętości plików lub spakowanych folderów w zakresie całej oferty do ilości 10 plików lub spakowanych folderów przy maksymalnej wielkości 150 MB.
18) Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez wykonawcę za pośrednictwem przycisku Wyślij wiadomość jako załączniki.
19) Wykonawca otrzyma powiadomienia tj. wiadomość email dotyczące komunikatów w sytuacji, gdy zamawiający opublikuje informacje publiczne lub spersonalizowaną

wiadomość zwaną prywatną korespondencją.

20) Warunkiem otrzymania powiadomień systemowych, o których mowa w ppkt. 19 jest wcześniejsze poinformowanie przez zamawiającego o postępowaniu, złożenie oferty jak i wystosowanie wiadomości przez wykonawcę w obrębie postępowania, na którą otrzyma odpowiedź.
21) Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
22) Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
23) Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po ich podpisaniu. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.
24) Za datę przekazania składanych dokumentów, oświadczeń, wniosków (innych niż wnioski o dopuszczenie do udziału w postępowaniu), zawiadomień, zapytań oraz przekazywanie informacji uznaje się kliknięcie przycisku Wyślij wiadomość, po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.
25) We wszelkiej korespondencji związanej z niniejszym postępowaniem zaleca się posługiwanie nazwą postępowania lub numerem referencyjnym niniejszego postępowania.
26) Zasady określone w niniejszym rozdziale nie dotyczą dokumentów składanych przez wykonawców przed podpisaniem umowy oraz zabezpieczenia należytego wykonania umowy, jeżeli są wymagane.

ROZDZIAŁ III Wspólne ubieganie się o udzielenie zamówienia publicznego

1. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy.
2. Pełnomocnictwo, o którym mowa w pkt 1 należy dołączyć do oferty.
3. Wszelką korespondencję w postępowaniu zamawiający kieruje do pełnomocnika.
4. Wspólnicy spółki cywilnej są wykonawcami wspólnie ubiegającymi się o udzielenie zamówienia i mają do nich zastosowanie zasady określone w pkt 1- 3.
5. Przed zawarciem umowy wykonawcy wspólnie ubiegający się o udzielenie zamówienia będą mieli obowiązek przedstawić zamawiającemu kopię umowy regulującej współpracę tych wykonawców, zawierającą, co najmniej:
   1) zobowiązanie do realizacji wspólnego przedsięwzięcia gospodarczego obejmującego swoim zakresem realizację przedmiotu zamówienia,
   2) określenie zakresu działania poszczególnych stron umowy,
   3) czas obowiązywania umowy, który nie może być krótszy, niż okres obejmujący realizację zamówienia.

ROZDZIAŁ IV Jawność postępowania. RODO

1. Zamawiający prowadzi i udostępnia protokół postępowania na zasadach określonych w ustawie oraz Rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 18 grudnia 2020 r. w sprawie protokołów postępowania oraz dokumentacji postępowania o udzielenie zamówienia publicznego.
2. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji,

jeżeli wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Zamawiający nie ponosi odpowiedzialności za ujawnienie ww. informacji, w sytuacji, gdy wykonawca odpowiednio nie wydzieli tych informacji i odpowiednio ich nie oznaczy. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy.

3. W sytuacji, gdy wykonawca zastrzeże w ofercie informacje, które nie stanowią tajemnicy przedsiębiorstwa lub są jawne na podstawie przepisów ustawy lub odrębnych przepisów, informacje te będą podlegały udostępnieniu na takich samych zasadach, jak pozostałe niezastrzeżone dokumenty.
4. Zamawiający udostępnia dane osobowe, o których mowa w art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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, ze zm.), zwanego dalej [11]RODO[11]. w celu umożliwienia korzystania za środków ochrony prawnej, o których mowa w ustawie, do upływu terminu na ich wniesienie.
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 danych) (Dz. U. UE L119 z dnia 4 maja 2016 r., str. 1); zwanym dalej **"RODO",** informujemy, że:
   1) administratorem Pani/Pana danych osobowych jest Powiatowa Stacja Sanitarno-Epidemiologiczna w Szczecinku.
   2) administrator wyznaczył Inspektora Danych Osobowych, z którym można się kontaktować pod adresem e-mail: **it.psse.szczecinek@sanepid.gov.pl**
   3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego, prowadzonym w trybie przetargu nieograniczonego.
   4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 74 p.z.p. oraz w stosunku do wybranego Wykonawcy pozostali Zamawiający, z którymi zostanie podpisana umowa.
   5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 p.z.p. przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
   6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach p.z.p., związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.
   7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
   8) posiada Pani/Pan:
      a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących (w przypadku, gdy skorzystanie z tego prawa wymagałoby po stronie administratora niewspółmiernie dużego wysiłku może zostać Pani/Pan zobowiązana do wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty

postępowania o udzielenie zamówienia publicznego lub konkursu albo sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia);

b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych *(skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą PZP oraz nie może naruszać integralności protokołu oraz jego załączników);*

c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania

d) danych osobowych z zastrzeżeniem okresu trwania postępowania o udzielenie zamówienia

e) publicznego lub konkursu oraz przypadków, o których mowa w art. 18 ust. 2 RODO *(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);*

f) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy **RODO;**

9) nie przysługuje Pani/Panu:
   a) w związku z art. 17 ust. 3 lit. b, d lube RODO prawo do usunięcia danych osobowych;
   b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
   c) na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO;
10) przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego na niezgodne z RODO przetwarzanie Pani/Pana danych osobowych przez administratora. Organem właściwym dla przedmiotowej skargi jest Urząd Ochrony Danych Osobowych w Warszawie.

ROZDZIAŁ V Warunki udziału w postępowaniu. Podstawy wykluczenia.

1. O udzielenie zamówienia może się ubiegać Wykonawca, który spełnia poniżej określony **warunek udziału w postępowaniu dotyczący zdolności technicznej lub zawodowej.** Zamawiający uzna, że Wykonawca spełnia warunek udziału w zakresie zdolności technicznej lub zawodowej, jeżeli Wykonawca wykaże że posiada odpowiednie normy zarządzania jakością:

a) **Certyfikat ISO 9001:2015 lub równoważny,**

b) **Certyfikat ISO-27001 lub równoważny,**

w zakresie świadczenia usług serwisowych (podmiot serwisujący).

W przypadku wspólnego ubiegania się Wykonawców o udzielenie zamówienia ww. warunek zostanie uznany za spełniony, jeżeli co najmniej jeden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia będzie posiadał wymagany powyżej certyfikat i zrealizuje zakres zamówienia, do którego realizacji ten certyfikat jest wymagany.

2. O udzielenie zamówienia może się ubiegać wykonawca, który nie podlega wykluczeniu z postępowania na podstawie:
   1) **art. 108 ust. 1** ustawy Pzp;
   2) **art. 109 ust. 1 pkt 4** ustawy Pzp;

3) **art. 7 ust. 1** ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz. U. z 2023 r., poz. 1497).

3. Wykonawca nie podlega wykluczeniu w okolicznościach, o których mowa w art. 108 ust.1pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 4, jeżeli udowodni zamawiającemu, że spełnił łącznie następujące przesłanki:
   1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;
   2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania, lub zamawiającym;
   3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:
      a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,
      b) zreorganizował personel,
      c) wdrożył system sprawozdawczości i kontroli,
      d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,
      e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.
4. Wykluczenie wykonawcy następuje przy uwzględnieniu przepisu art. 111 ustawy Pzp.
5. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, uzna za wystarczające dowody przedstawione na podstawie ust. 3 powyżej.
6. Zamawiający może wykluczyć wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

ROZDZIAŁ VI Wymagane dokumenty - podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne oświadczenia

1. **WYKAZ WYMAGANYCH OŚWIADCZEŃ I DOKUMENTÓW <u>SKŁADANYCH WRAZ Z OFERTĄ</u>:**
   1) **Formularz oferty**, według wzoru stanowiącego **załącznik nr 1 do SWZ**;
   2) **Wykaz oferowanego sprzętu wraz ze wskazaniem** w tym wykazie oznaczeń identyfikujących oferowany przedmiot zamówienia *(należy podać oferowane parametry – pod rygorem odrzucenia oferty);*
   3) W celu potwierdzenia, że osoba działająca w imieniu wykonawcy, wykonawcy wspólnie ubiegającego się o udzielenie zamówienia, jest umocowana do jego reprezentowania wykonawca składa wraz z ofertą:
      a) **odpis lub informację z Krajowego Rejestru Sądowego, Centralnej Ewidencji** i **Informacji o Działalności Gospodarczej lub innego właściwego rejestru.** *W przypadku wykonawców wspólnie ubiegających się o zamówienie, każdy z wykonawców zobowiązany jest do złożenia ww. dokumentów*
      Uwaga: wykonawca nie jest zobowiązany do złożenia ww. dokumentów, jeżeli zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz

danych, o ile wykonawca wskazał odpowiednio w **załączniku nr 1** do SWZ (Formularz ofertowy) dane umożliwiające dostęp do tych dokumentów;

b) **pełnomocnictwa** lub inne dokumenty potwierdzające umocowanie do reprezentowania (odpowiednio: wykonawcy, wykonawców wspólnie ubiegających się o udzielenie zamówienia), jeżeli w jego imieniu działa osoba, której umocowanie do reprezentowania nie wynika z dokumentów, o których mowa w pkt 1 ppkt 1 lit. a) powyżej;

4) **Przedmiotowe środki dowodowe,** tj. odpowiednie normy zarządzania jakością **w zakresie serwera do instalacji systemu centralnego logowania z systemem uwierzytelniania, autoryzacją i kontrolą dostępu:**

a) certyfikat ISO-9001:2015, ISO-50001 oraz ISO-14001 lub certyfikat równoważny, na oferowany serwer,

b) certyfikat ISO 1043-4 lub równoważny, dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr,
oraz

c) oświadczenie, że oferowany serwer spełnia wymogi określone w Dyrektywie RoHS (dyrektywa 2002/95/WE), wprowadzającej ograniczenia stosowania niektórych niebezpiecznych substancji i materiałów w sprzęcie elektrycznym i elektronicznym.

UWAGA! Wszystkie przedmiotowe środki dowodowe muszą być złożone w języku polskim.

Zgodnie z art. 107 ust. 2 ustawy Prawo zamówień publicznych, jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.

5) W celu potwierdzenia braku podstaw wykluczenia wykonawca składa wraz z ofertą **oświadczenie wykonawcy o braku podstaw wykluczenia** wykonawcy, według wzoru stanowiącego **załącznik nr 2** do SWZ.
W przypadku wspólnego ubiegania się wykonawców o udzielenie zamówienia ww. dokument składa każdy z wykonawców wspólnie ubiegających się o zamówienie.

6) W celu potwierdzenia spełnienia warunków udziału w postępowaniu Wykonawca składa wraz z ofertą **oświadczenie Wykonawcy o spełnieniu warunków udziału w postępowaniu**, według wzoru stanowiącego **załącznik nr 3 do SWZ**.
W przypadku wspólnego ubiegania się Wykonawców o udzielenie zamówienia ww. dokument składa pełnomocnik Wykonawców wspólnie ubiegających się o zamówienie.

7) oświadczenie Wykonawców wspólnie ubiegających się o udzielenie zamówienia wskazujące, które dostawy wykonają poszczególni Wykonawcy, według wzoru stanowiącego **załącznik nr 4 do SWZ.**
Ww. dokument należy złożyć w przypadku wspólnego ubiegania się Wykonawców o udzielenie zamówienia.

8) **zobowiązanie podmiotu udostępniającego zasoby** według wzoru stanowiącego **załącznik nr 5 do SWZ**, do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia wraz z oświadczeniem podmiotu udostępniającego zasoby, potwierdzającym brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby, według wzoru przekazanego przez Zamawiającego. Zobowiązanie podmiotu udostępniającego zasoby może być zastąpione innym podmiotowym środkiem dowodowym potwierdzającym, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tego podmiotu.
Ww. zobowiązanie należy złożyć tylko wtedy, gdy Wykonawca polega na zdolnościach

lub sytuacji podmiotu udostępniającego zasoby.

2. WYKAZ WYMAGANYCH OŚWIADCZEŃ I DOKUMENTÓW SKŁADANYCH NA WEZWANIE ZAMAWIAJĄCEGO:

1) **W celu potwierdzenia spełnienia warunku udziału w postępowaniu** Zamawiający wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia odpowiednich norm zarządzania jakością, tj.:
   a) Certyfikat ISO 9001:2015 lub równoważny,
   b) Certyfikat ISO-27001 lub równoważny,
   w zakresie świadczenia usług serwisowych (podmiot serwisujący).
2) **W celu potwierdzenia braku podstaw wykluczenia z postępowania** Zamawiający wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia podmiotowych środków dowodowych tj. odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt. 4 ustawy Pzp, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;

   W przypadku składania oferty wspólnej ww. dokument składa każdy z wykonawców składających ofertę wspólną.
   Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych (odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej), jeżeli może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile wykonawca wskazał w załączniku nr 2 do SWZ dane umożliwiające dostęp do tych dokumentów.
   UWAGA: Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast odpisu lub informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury. Dokument powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.

   Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów jw., 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 lub miejsce zamieszkania ma osoba, której dokument miał dotyczyć, 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. Dokument powinien być wystawiony nie wcześniej niż 3 miesiące przed jego złożeniem.

3. WYMAGANIA DODATKOWE:

1) Wykonawca składa Ofertę sporządzoną na Formularzu ofertowym, stanowiącym **załącznik nr 1** do SWZ.

2) **Wykonawca wraz z ofertą zobowiązany jest do złożenia Wykazu oferowanego sprzętu (stanowiącego jednocześnie Opis przedmiotu zamówienia)** oraz do **wskazania** w ww. wykazie oznaczeń identyfikujących oferowany przedmiot zamówienia - **należy podać oferowane parametry** (nie dopuszcza się stwierdzeń TAK, OK itp.).
UWAGA! Brak wskazania oznaczeń identyfikujących oferowany przedmiot zamówienia, w celu jego weryfikacji przez Zamawiającego, będzie skutkować odrzuceniem oferty Wykonawcy.

3) Oferta (dokumenty tworzące ofertę) musi być podpisana przez osoby upoważnione do reprezentowania wykonawcy, zgodnie z formą reprezentacji wykonawcy określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej wykonawcy albo przez umocowanego przedstawiciela wykonawcy. W związku z powyższym wykonawca składa wraz z ofertą dokumenty, z których wynika umocowanie do podpisania oferty oraz wszelkich dokumentów/oświadczeń składanych wraz z ofertą (w przypadku pełnomocnictw - oryginał lub poświadczona notarialnie kopia) chyba, że zamawiający 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, a wykonawca wskazał w ofercie odpowiedni adres internetowy, na którym zamawiający może pobrać dokument. W przypadku wskazania przez wykonawcę dostępności ww. dokumentu w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, zamawiający pobiera je samodzielnie. W przypadku braku podania w ofercie ww. adresu, zamawiający może pobrać ww. dokumenty w formie elektronicznej, o ile te są dostępne w ogólnodostępnych i bezpłatnych bazach danych.

4) W przypadku wspólnego ubiegania się o udzielenie zamówienia wykonawców występujących wspólnie (dotyczy również spółki cywilnej) - z ofertą należy złożyć pełnomocnictwo do reprezentowania w postępowaniu o udzielenie zamówienia publicznego albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego (oryginał lub poświadczona notarialnie kopia).

5) Postępowanie o udzielnie zamówienia prowadzi się w języku polskim. **Dokumenty lub oświadczenia sporządzone w języku obcym składane są wraz z tłumaczeniem na język polski. Zasada ta rozciąga się na składane w toku postępowania dokumenty, wyjaśnienia, oświadczenia, wnioski, zawiadomienia oraz informacje itp.**

6) W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia (spółki cywilne, konsorcja), żaden z nich nie może podlegać wykluczeniu na podstawie art. 108 ust. 1 i 109 ust. 1 pkt 4 ustawy Pzp, a także art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę.

7) Zamawiający nie wzywa 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 wskazał w oświadczeniu o braku podstaw wykluczenia **(załącznik nr 2** do SWZ), dane umożliwiające dostęp do tych środków.

8) Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
9) W zakresie nie uregulowanym SWZ, zastosowanie mają przepisy Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy.
10) Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, o których mowa w niniejszej SWZ sporządza się w formie elektronicznej (podpisane kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym w sposób określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie.

ROZDZIAŁ VII Opis sposobu przygotowania oferty

1. Wykonawca ma prawo złożyć tylko jedną ofertę.
2. Zaleca się, aby przed rozpoczęciem wypełniania Formularza składania oferty wykonawca zalogował się na Platformie, a jeżeli nie posiada konta, założył bezpłatne konto. W przeciwnym wypadku wykonawca będzie miał ograniczone funkcjonalności, np. brak widoku wiadomości prywatnych od zamawiającego w systemie lub wycofania oferty lub wniosku bez kontaktu z Centrum Wsparcia Klienta.
3. Konto wykonawcy tworzone jest tylko raz, w kolejnych postępowaniach wykorzystuje się już istniejące konto.
4. Wykonawca składa ofertę za pośrednictwem Formularza składania oferty dostępnego na platformazakupowa.pl w konkretnym postępowaniu w sprawie udzielenia zamówienia publicznego.
5. Jeżeli zamawiający w ogłoszeniu o zamówieniu czy SWZ nie zaznaczył inaczej, wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać załączone w osobnym miejscu w kroku 1 składania oferty przeznaczonym na zamieszczenie tajemnicy przedsiębiorstwa.
6. Zgodnie z§ 4. ust 1. 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 wymaga się, aby dokumenty zawierające informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, wykonawca przekazał w wydzielonym i odpowiednio oznaczonym pliku. UWAGA: W przypadku, gdy oferta, oświadczenia lub dokumenty będzie zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, Wykonawca, nie później niż w terminie składania ofert, powinien w sposób niebudzący wątpliwości zastrzec, że nie mogą być one udostępniane oraz wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Nie mogą stanowić tajemnicy przedsiębiorstwa informacje podawane do wiadomości podczas otwarcia ofert, o których mowa w rozdziale XII pkt. 9 SWZ. Zastrzeżenie informacji, danych, dokumentów i oświadczeń niestanowiących tajemnicy przedsiębiorstwa w rozumieniu przepisów o nieuczciwej konkurencji

spowoduje ich odtajnienie przez Zamawiającego.

7. Do oferty należy dołączyć wszystkie wymagane w Ogłoszeniu i SWZ dokumenty i oświadczenia.
8. Po wypełnieniu Formularza składania oferty i załadowaniu wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania".
9. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
10. Wykonawca po upływie terminu składania ofert nie może dokonać zmiany złożonej oferty.
11. Zamawiający nie ponosi odpowiedzialności za nieprawidłowe lub nieterminowe złożenie oferty. Zaleca się, aby założyć profil wykonawcy i rozpocząć składanie oferty z odpowiednim wyprzedzeniem.
12. W przypadku składania oferty przez wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum) - Pełnomocnikiem konsorcjum jest wykonawca, który zaloguje się na swoim profilu wykonawcy i składając ofertę w zakładce „wykonawcy" doda pozostałych Wykonawców wpisując ich dane.
13. Oferta musi być złożona przed upływem terminu składania ofert.
14. Wykonawca złoży ofertę zgodnie z wymaganiami SWZ.
15. W formularzu ofertowym wykonawca wskazuje, wyłącznie do celów statystycznych, czy jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem lub innym podmiotem. I tak zgodnie z przepisami ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców:
    1) **mikroprzedsiębiorca** - to przedsiębiorca, który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a) zatrudniał średniorocznie mniej niż 10 pracowników oraz b)osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 2 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 milionów euro;
    2) **mały przedsiębiorca** - to przedsiębiorca, który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a) zatrudniał średniorocznie mniej niż 50 pracowników oraz b) osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 10 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 10 milionów euro, i który nie jest mikroprzedsiębiorcą,
    3) **średni przedsiębiorca** - to przedsiębiorca, który w co najmniej jednym roku z dwóch ostatnich lat obrotowych spełniał łącznie następujące warunki: a)zatrudniał średniorocznie mniej niż 250 pracowników oraz b)osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 43 milionów euro, i który nie jest mikro przedsiębiorcą ani małym przedsiębiorcą.

    Uwaga: Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczącego definicji przedsiębiorstw mikro, małych i średnich (notyfikowane jako dokument nr C{2003) 1422) (Dz.U. L 124 z 20.5.2003, s. 36-41).

ROZDZIAŁ VIII Termin wykonania zamówienia

Termin wykonania przedmiotu zamówienia: - **do 14 dni od dnia zawarcia umowy.**

ROZDZIAŁ IX Wadium

Zamawiający nie wymaga wniesienia wadium w niniejszym postępowaniu.

ROZDZIAŁ X Wyjaśnienia treści SWZ i jej modyfikacja

1. Wykonawca może zwrócić się do zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na **2 dni** przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynie do zamawiającego nie później niż na **4 dni** przed upływem terminu składania ofert.
2. Zaleca się, aby wnioski o wyjaśnienie treści SWZ były przekazywane w wersji edytowalnej.
3. Treść pytań wraz z wyjaśnieniami zamawiający udostępnia na stronie internetowej prowadzonego postępowania bez ujawniania źródła zapytania.
4. W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ zamawiający udostępnia na stronie internetowej prowadzonego postępowania.
5. Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem **platformazakupowa.pl** poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

ROZDZIAŁ XI Sposób obliczenia ceny oferty

1. Wykonawca w formularzu ofertowym wskazuje:
   1) wartość oferty brutto (zł),
   2) stawkę podatku VAT(%),

   zgodnie z treścią Formularza ofertowego.
2. Wartość oferty brutto podlega ocenie w ramach kryterium oceny ofert „cena" - rozdział XIII SWZ.
3. Cena oferty musi uwzględniać całość ponoszonego przez Zamawiającego wydatku na sfinansowanie zamówienia i stanowi jednocześnie maksymalny koszt Zamawiającego w związku z realizacją zamówienia. Cena ta nie podlega negocjacjom czy zmianie w toku postępowania z zastrzeżeniem art. 223 ust. 2 ustawy Pzp.
4. Cena oferty brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia, zgodnie z Opisem przedmiotu zamówienia stanowiącym załącznik nr 3 do SWZ, w tym ryzyko Wykonawcy z tytułu oszacowania wszelkich kosztów związanych z realizacją zamówienia, a także oddziaływania innych czynników mających lub mogących mieć wpływ na koszty. W cenie oferty uwzględnić należy wszelkie należności publiczno-prawne wykonawcy, w tym podatek od towarów i usług (podatek VAT), jeżeli na podstawie obowiązujących w Polsce przepisów prawa, w tym przepisów obowiązującej ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.
5. Cenę oferty brutto należy podać w złotych w kwocie brutto w odniesieniu do całego przedmiotu zamówienia, z dokładnością do dwóch miejsc po przecinku (zgodnie z matematycznymi zasadami zaokrągleń).
6. Zamawiający nie przewiduje rozliczeń w walucie obcej.
7. Wyliczona cena oferty brutto będzie służyć do rozliczenia w trakcie realizacji zamówienia.
8. Jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć.
9. W ofercie, o której mowa w pkt 8, Wykonawca ma obowiązek:

1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;
2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez
4) kwoty podatku;
5) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

Powyższe informacje zaleca się podać na odrębnym załączanym do oferty dokumencie, przygotowanym przez Wykonawcę. Brak załączenia do oferty tego dokumentu (o ile Wykonawca nie wskazał takiej informacji w dokumentach swojej oferty) oznacza, iż wybór oferty Wykonawcy nie prowadzi do powstania u Zamawiającego obowiązku, o którym mowa w pkt 8.

ROZDZIAŁ XII Składanie i otwarcie ofert

1. Ofertę składa się pod **rygorem nieważności w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**
2. Ofertę wraz z wymaganymi oświadczeniami oraz dokumentami należy złożyć za pośrednictwem Platformy w terminie **do dnia 03.11.2023 r., do godz. 09:00.**
3. Otwarcie ofert odbędzie się **w dniu 03.11.2023 r., o godz. 09:15.**
4. Za datę przekazania oferty przyjmuje się datę jej przekazania na Platformę.
5. Wykonawca pozostaje związany ofertą przez okres nie dłuższy niż 30 dni tj. **do dnia 02.12.2023 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert. Szczegółowe informacje dotyczące terminu związania ofertą określono w przepisach m.in. art. 307 ustawy Pzp.
6. Otwarcie ofert nastąpi przy użyciu systemu teleinformatycznego. W przypadku awarii tego systemu, która spowoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
7. W sytuacji, o której mowa w pkt 6 zamawiający zamieści na stronie internetowej prowadzonego postępowania informację o zmianie terminu otwarcia ofert.
8. Zamawiający najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
9. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje, o których mowa w art. 222 ust. 5 ustawy Pzp.

ROZDZIAŁ XII Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów i sposobu oceny ofert

1. **Wybór oferty najkorzystniejszej zostanie dokonany według następujących kryteriów oceny ofert:**

Lp.	Kryterium	Waga kryterium	Liczba punktów
1	**Cena**	**80%**	**80 pkt**
2	**Okres gwarancji**	**20%**	**20 pkt**

1) ,,Cena" - waga kryterium 80%.
Sposób przyznania punktów w kryterium „Cena": najniższa cena ofertowa brutto spośród ofert niepodlegających odrzuceniu

$$C = \frac{\text{cena ofertowa brutto w ofercie ocenianej}}{\text{najniższa cena ofertowa brutto spośród ofert niepodlegających odrzuceniu}} \times 100 \text{ pkt} \times 80\%$$

Podstawą przyznania punktów w kryterium „cena" będzie cena oferty brutto podana przez Wykonawcę w Formularzu Ofertowym. Cena oferty brutto musi uwzględniać wszelkie koszty jakie Wykonawca poniesie w związku z realizacją przedmiotu zamówienia. W tym kryterium Wykonawca może uzyskać maksymalnie 80 punktów.

2) ,,Okres gwarancji" - waga kryterium 20%
Kryterium „Okres gwarancji" będzie rozpatrywany na podstawie okresu gwarancji zadeklarowanego przez Wykonawcę na Formularzu Ofertowym.

Zamawiający wymaga, aby **minimalny okres gwarancji wynosił 60 miesięcy** od dnia podpisania protokołu odbioru przedmiotu umowy.

Liczba punktów w ramach kryterium „Okres gwarancji" zostanie przyznana w następujący sposób:

- 60 miesięcy - 0 pkt
- 84 miesiące -10 pkt
- 85 i więcej - 20 pkt

W tym kryterium Wykonawca może uzyskać maksymalnie 20 punktów.

UWAGA:
W przypadku błędnego wypełnienia formularza w zakresie okresu gwarancji, tj. braku wskazania okresu gwarancji, wskazania dwóch punktów w zakresie gwarancji, bądź wskazanie innego okresu gwarancji, niż 60 m-cy/ 84 m-ce/ lub 85 i więcej, oferta otrzyma w tym kryterium 0 pkt, a okres gwarancji zostanie przyjęty jako minimalny tj. 60 miesięcy.

2. Zamawiający oceni oferty sumując punkty uzyskane z kryteriów zgodnie z wzorem:

liczba punktów uzyskana przez ofertę badaną=
liczba punktów uzyskana w kryterium „Cena"
+ liczba punktów uzyskana w kryterium „Okres gwarancji"

3. Zamawiający wybierze ofertę, która uzyskała najwięcej punktów, spełniającą wymagania określone w SWZ.

ROZDZIAŁ XIV Zawarcie umowy oraz informacja o formalnościach jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Projektowane postanowienia umowy, które zostaną wprowadzone do treści tej umowy zawarte są we wzorze umowy stanowiącym **załącznik nr 7** do SWZ. **Wykonawca ma obowiązek zawrzeć umowę zgodnie z tymi postanowieniami.**
2. Zakres świadczenia Wykonawcy wynikający z umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
3. Zamawiający przewiduje możliwość zmiany zawartej umowy w stosunku do treści wybranej oferty w zakresie uregulowanym w art. 454-455 PZP oraz wskazanym we Wzorze Umowy, stanowiącym **Załącznik nr 7** do SWZ.
4. Zmiana umowy wymaga dla swej ważności zachowania formy pisemnej pod rygorem nieważności.
5. Przed zawarciem umowy Wykonawca zobowiązany jest do przedłożenia Zamawiającemu:
   1) pełnomocnictw, chyba, że w ofercie znajdują się dokumenty lub pełnomocnictwa upoważniające osoby lub osobę do podpisania umowy w sprawie udzielenia zamówienia publicznego w imieniu wykonawcy lub w imieniu wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego,
   2) umów z ewentualnymi aneksami regulujących współpracę między wykonawcami występującymi wspólnie. Umowa regulująca współpracę tych wykonawców winna zawierać co najmniej:
      a) zobowiązanie do realizacji wspólnego przedsięwzięcia gospodarczego obejmującego swoim zakresem realizację przedmiotu zamówienia,
      b) określenie zakresu działania poszczególnych stron umowy,
      c) czas obowiązywania umowy, który nie może być krótszy, niż okres obejmujący realizację zamówienia.

ROZDZIAŁ XV Zabezpieczenie należytego wykonania umowy

Wykonawca nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XVI Pouczenie o środkach ochrony prawnej

1. Wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy, przysługują

środki ochrony prawnej (odwołanie i skarga) przewidziane w Dziale IX Ustawy Pzp.

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 ustawy, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
   1) niezgodną z przepisami ustawy czynność zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
   2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której zamawiający był obowiązany na podstawie ustawy;
   3) zaniechanie przeprowadzenia postępowania o udzielenie zamówienia, mimo że zamawiający był do tego obowiązany.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej, zwanej dalej Izbą. Odwołujący przekazuje zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu.
5. Domniemywa się, że zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przekazanie odpowiednio odwołania albo jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.
6. Odwołanie wnosi się w terminie:
   1) 5 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej,
   2) 10 dni od dnia przekazania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana w sposób inny niż określony w ppkt 1).
7. Odwołanie wobec treści ogłoszenia wszczynającego postępowanie o udzielenie zamówienia lub wobec treści dokumentów zamówienia wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub dokumentów zamówienia na stronie internetowej prowadzonego postępowania.
8. Odwołanie w przypadkach innych niż określone w pkt 6 i 7 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
9. Jeżeli zamawiający mimo takiego obowiązku nie przesłał wykonawcy zawiadomienia o wyborze najkorzystniejszej oferty, odwołanie wnosi się nie później niż w terminie:
   1) 15 dni od dnia zamieszczenia w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania;
   2) miesiąca od dnia zawarcia umowy, jeżeli zamawiający nie zamieścił w Biuletynie Zamówień Publicznych ogłoszenia o wyniku postępowania.
10. Odwołanie zawiera elementy wskazane w art. 516 ustawy.
11. Na orzeczenie Izby oraz postanowienie Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.
12. W postępowaniu toczącym się wskutek wniesienia skargi stosuje się odpowiednio przepisy ustawy z dnia 17 listopada 1964r. - Kodeks postępowania cywilnego o apelacji, jeżeli przepisy Działu IX ustawy nie stanowią inaczej.
13. Skargę wnosi się do Sądu Okręgowego w Warszawie - sądu zamówień publicznych.
14. Skargę wnosi się za pośrednictwem Prezesa Izby, w terminie 14 dni od dnia doręczenia orzeczenia Izby lub postanowienia Prezesa Izby, o którym mowa w art. 519 ust. 1 ustawy, przesyłając jednocześnie jej odpis przeciwnikowi skargi. Złożenie skargi w placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. - Prawo pocztowe jest równoznaczne z jej wniesieniem.
15. Skarga powinna czynić zadość wymaganiom przewidzianym dla pisma procesowego oraz zawierać

oznaczenie zaskarżonego orzeczenia, ze wskazaniem, czy jest ono zaskarżone w całości, czy w części, przytoczenie zarzutów, zwięzłe ich uzasadnienie, wskazanie dowodów, a także wniosek o uchylenie orzeczenia lub o zmianę orzeczenia w całości lub w części, z zaznaczeniem zakresu żądanej zmiany.

ROZDZIAŁ XVI Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych zadań dotyczących prac związanych z rozmieszczeniem i instalacją.

ROZDZIAŁ XVII Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest **Dostawa systemu bezpieczeństwa (UTM) centralnego systemu logowania, system centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami.**
2. Wykonawca w ramach realizacji zamówienia publicznego zobowiązany jest do przeprowadzenia szkoleń, o których mowa w opisie przedmiotu zamówienia, stanowiącego **załącznik nr 6** do SWZ.
3. Wykonawca, w ramach realizacji zamówienia, musi dysponować min. dwoma inżynierami, zgodnie z OPZ, posiadającymi certyfikaty oferowanej przez Wykonawcę technologii (na żądanie Zamawiającego, Wykonawca zobowiązany będzie podać numery certyfikatów, w celu weryfikacji, poprzez wprowadzenie go na dedykowanej stronie internetowej jednostki certyfikującej (producenta rozwiązania).
4. **Wykonawca wraz z ofertą przedłoży przedmiotowe środki dowodowe, w zakresie serwera do instalacji systemu centralnego logowania z systemem uwierzytelniania, autoryzacją i kontrolą dostępu:**
   d) certyfikat ISO-9001:2015, ISO-50001 oraz ISO-14001 lub certyfikat równoważny, na oferowany serwer,
   e) certyfikat ISO 1043-4 lub równoważny, dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr,
   f) oświadczenia, że oferowany serwer spełnia wymogi określone w Dyrektywie RoHS (dyrektywa 2002/95/WE), wprowadzającej ograniczenia stosowania niektórych niebezpiecznych substancji i materiałów w sprzęcie elektrycznym i elektronicznym.
5. Szczegółowy opis oraz sposób realizacji zamówienia zawiera opis przedmiotu zamówienia, stanowiący Załącznik nr 6 do SWZ.
6. Wspólny Słownik Zamówień CPV:
   48000000-8 Pakiety oprogramowania i systemy informatyczne
   Przedmiot zamówienia nie został podzielony na części. Zamawiający nie dopuszcza składania ofert częściowych.
   Ze względów organizacyjnych i technicznych oraz jednorodności przedmiotu zamówienia, Zamawiający nie dokonał podziału zamówienia na części. Celem wprowadzenia możliwości podziału zamówień na części jest zwiększenie udziału sektora małych i średnich przedsiębiorstw (MŚP) w rynku zamówień publicznych. Brak podziału zamówienia na części nie skutkuje brakiem możliwości złożenia oferty w niniejszym postępowaniu przez małych i średnich przedsiębiorców.
7. Zamawiający nie przewiduje udzielania zamówień, o których mowa w art. 214 ust. 1 pkt 8 p.z.p.
8. Wykonawca złoży ofertę zgodnie z Formularzem Ofertowym Stanowiącym załącznik nr 1 do SWZ.
9. Przedmiot zamówienia zostanie zrealizowany zgodnie ze wzorem umowy, stanowiącym załącznik nr 7 do SWZ oraz opisem przedmiotu zamówienia, zawartym w załączniku nr 6 do SWZ.
10. Zamawiający zastrzega, że wszędzie tam, gdzie w treści niniejszej SWZ oraz załącznikach do niej, zostały w opisie przedmiotu wskazane znaki towarowe, patenty lub pochodzenie, źródła lub szczególne procesy, które charakteryzują produkty lub usługi dostarczane przez konkretnego wykonawcę - Zamawiający dopuszcza metody, materiały, urządzenia, technologie itp. równoważne do przedstawionych w opisie przedmiotu zamówienia, rozumiane jako wykonane przez dowolnych producentów przy zachowaniu

identycznych lub lepszych parametrów technicznych i walorów użytkowych oraz w pełni kompatybilnych z resztą urządzeń pod warunkiem, iż spełnią one te same właściwości techniczne oraz na etapie realizacji uzyskają akceptację Zamawiającego. Decyzje Zamawiającego w tym zakresie oparte będą na wymaganiach sformułowanych w dokumentach zamówienia, umowie, a także normach i wytycznych. Parametry wskazanego standardu określają minimalne warunki techniczne, eksploatacyjne, użytkowe, jakościowe i funkcjonalne, jakie ma spełniać przedmiot zamówienia. Wskazane marki, nazwy producenta, znaki towarowe, patenty, pochodzenie, źródła lub szczególne procesy, które charakteryzują produkty - służą ustaleniu pożądanego standardu wykonania i określeniu właściwości, wymogów technicznych produktu, metody, materiałów, urządzeń, technologii itp. założonych w treści SWZ oraz załącznikach.

11. Dopuszcza się możliwość zastosowania rozwiązań równoważnych do wszystkich elementów przedmiotu zamówienia, które mogły zostać opisane przy użyciu norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy Pzp.
12. Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez Zamawiającego.
13. Wykonawca zrealizuje niezbędne czynności i poniesie wszelkie koszty związane z realizacją zamówienia.
14. Realizacja zamówienia podlega prawu polskiemu, w tym w szczególności ustawie Kodeks cywilny i ustawie Prawo zamówień publicznych.

Signature Not Verified

Dokument podpisany przez Wiesław Kulik; PSSE Szczecinek
Data: 2023.10.25 12:17:08 CEST

Dyrektor
Powiatowej Stacji Sanitarno - Epidemiologicznej
w Szczecinku
Wiesław Kulik
/dokument podpisany elektronicznie/

Załącznik nr 1 do SWZ/ nr 2 do umowy

FORMULARZ OFERTOWY

Informacje dotyczące wykonawcy *{Identyfikacja wykonawcy):*	**Odpowiedź:** *(wypełnia wykonawca)*
Nazwa i adres wykonawcy[1]:	
Numer NIP: Numer REGON[2]:	[.....] [.....]
Dane teleadresowe wykonawcy[3]: Telefon: Adres e-mail:	 [.....] [.....]
Rodzaj Wykonawcy *(wybrać odpowiednie)*[3]	O mikroprzedsiębiorstwo O mate przedsiębiorstwo O średnie przedsiębiorstwo O jednoosobowa działalność gospodarcza O osoba fizyczna nieprowadząca działalności gospodarczej O inny rodzaj
Dane osoby upoważnionej do reprezentowania wykonawcy w postępowaniu: Imię i nazwisko: Stanowisko: Podstawa umocowania:	 [.....] [.....] [....,]
Czy dokumentacja, z której wynika sposób reprezentacji wykonawcy (np. organ uprawniony do reprezentacji podmiotu) można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych[4]: Jeżeli powyższe dane są dostępne w formie elektronicznej, proszę wskazać dane niezbędne do ich pobrania:	[ ] Tak, można uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych [ ] Nie (np. adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji, identyfikator wydruku}: [.....]

[1] *W przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich członków konsorcjum lub spółki cywilnej.*

[2] *W przypadku składania oferty przez podmioty występujące wspólnie numer NIP i REGON wszystkich członków konsorcjum lub spółki cywilnej.*

[3] *Patrz rozdział VII pkt. 15 SWZ.*

W odpowiedzi na ogłoszenie o zamówieniu prowadzonym w trybie podstawowym bez negocjacji pn.: **„Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, system centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami"** niniejszym:

1. **SKŁADAMY** ofertę na wykonanie przedmiotu zamówienia zgodnie ze SWZ.
2. **OŚWIADCZAMY,** że zapoznaliśmy się ze SWZ i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
3. **OFERUJEMY** wykonanie przedmiotu zamówienia, zgodnie z Opisem przedmiotu zamówienia, za cenę ofertową w tym:
   1) **System bezpieczeństwa (UTM) – 2 szt.**

…… **złotych brutto, w tym…….% podatku VAT,**

   2) **Centralny system logowania – 1 szt.**

…… **złotych brutto, w tym…….% podatku VAT,**

   3) **System centralnego zarządzania urządzeniami bezpieczeństwa – 1 szt.**

…… **złotych brutto, w tym…….% podatku VAT.**

4. **OŚWIADCZAMY,** że udzielamy gwarancji na okres: *(uzupełnić poprzez wpisanie „X" w odpowiednią kratkę):*
   □ **- 60 miesięcy,** licząc od dnia podpisania protokołu odbioru przedmiotu umowy
   □ **- 84 miesiące,** licząc od dnia podpisania protokołu odbioru przedmiotu umowy
   □ **- 85 miesięcy i więcej,** licząc od dnia podpisania protokołu odbioru przedmiotu umowy
5. **OŚWIADCZAMY**, **<u>że w przypadku zaistnienia wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania)</u>** znajdują zastosowanie przepisy prawa dotyczące produktów podwójnego zastosowania, a treść tych regulacji jest mi znana, w szczególności Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z dnia 20 maja 2021 r. ustanawiające unijny system kontroli wywozu, pośrednictwa, pomocy technicznej, tranzytu i transferu produktów podwójnego zastosowania oraz Ustawa z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Ustawa z 29 listopada 2000 r.).
6. **UWAŻAMY SIĘ** za związanych niniejszą ofertą przez czas wskazany w SWZ.
7. **OŚWIADCZAMY,** że zapoznaliśmy się ze wzorem umowy i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w SWZ i w terminie wyznaczonym przez Zamawiającego.
8. **OŚWIADCZAMY,** że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[5] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu[6].
9. **OŚWIADCZAMY,** iż informacje i dokumenty zawarte na stronach nr od ___ do_____stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, co wykazaliśmy w załączniku nr_ do oferty i zastrzegamy, że nie mogą być one udostępniane.

   ---
10. **OŚWIADCZAMY,** że sposób reprezentacji spółki/ konsorcjum dla potrzeb niniejszego zamówienia jest następujący *(niepotrzebne skreślić):*

(Wypełniają jedynie przedsiębiorcy składający wspólną ofertę - spółki cywilne lub konsorcja)

11. **WSZELKĄ KORESPONDENCJĘ w sprawie niniejszego postępowania należy kierować na poniższy adres:**

---

tel. _____ e-mail: _____

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

'skreślić w przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO

Należy podpisać *zgodnie z Rozporządzeniem 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.*

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 2 do SWZ

OŚWIADCZENIE WYKONAWCY DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Ja (My), niżej podpisany (ni) .....
działając w imieniu i na rzecz:

.....
(pełna nazwa wykonawcy)

.....
(adres siedziby wykonawcy)

przystępując do postępowania o udzielenie zamówienia publicznego, w trybie podstawowym, pod nazwą **„Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, systemu centralnego zarządzania urządzeniami i bezpieczeństwa wraz ze szkoleniami"** zgodnie z ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 ze zm.), oświadczam, co następuje:

OŚWIADCZENIE WYKONAWCY

1) Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 oraz art. 109 ust. 1 pkt. 4 ustawy Pzp.
2) Oświadczam, że na dzień składania ofert nie podlegam wykluczeniu z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2012 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
3)

PROCEDURA SAMOOCZYSZCZENIA
(uzupełnić jeśli dotyczy)

Oświadczam, że na dzień składania ofert, zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ..... ustawy Pzp *(podać mająca zastosowanie podstawę wykluczenia spośród wymienionych w* art. 108 ust. 1 oraz art. 109 ust. 1 pkt. 4 ustawy Pzp). Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp.
podjąłem następujące środki naprawcze:..... *{opisać podjęte środki naprawcze)*

INFORMACJA DOTYCZĄCA DOSTĘPU DO BEZPŁATNYCH I OGÓLNODOSTĘPNYCH BAZ DANYCH

Ja/my niżej podpisany(-a)(-i) aby wyrażam(-y) zgodę aby Zamawiający uzyskał dostęp do dokumentów potwierdzających informacje, które zostały przedstawione w **załączniku nr 2** do SWZ na potrzeby niniejszego postępowania, między innymi w zakresie podstawy wykluczenia o której mowa w art. 109 ust. 1 pkt. 4 ustawy

Pzp,

Dokumenty te pobrać można pod adresami:
- odpis lub informacja z Krajowego Rejestru Sądowego: **https://ems.ms.gov.pl/**
- odpis lub informacja z Centralnej Ewidencji i Informacji o Działalności Gospodarczej: **https://prod.ceidg.gov.pl;**

W przypadku, gdy dokumenty te dostępne są pod innymi adresami niż powyżej podać należy np. adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji, identyfikator wydruku:

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI

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

Należy podpisać *zgodnie z Rozporządzeniem 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.*

Załącznik nr 3 do SWZ

OŚWIADCZENIE WYKONAWCY O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU (składane na podstawie art. 125 ust. 1 ustawy PZP)

Działając w imieniu i na rzecz :

.....
(pełna nazwa wykonawcy)

.....
(adres siedziby wykonawcy)

w odpowiedzi na ogłoszenie o postępowaniu na:

„Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, systemu centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami"

oświadczam, że wykonawca, którego reprezentuję spełnia warunki udziału w postępowaniu określone w Rozdziale V pkt 1 SWZ.

Należy podpisać *zgodnie z Rozporządzeniem 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.*

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 4 do SWZ

OŚWIADCZENIE WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA (składane na podstawie art. 117 ust. 4 ustawy)

Działając w imieniu i na rzecz : .....

.....

(pełna nazwa Wykonawcy)

.....

(adres siedziby Wykonawcy)

w odpowiedzi na ogłoszenie o postępowaniu na:

„Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, systemu centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami"

oświadczamy, że następujący zakres zamówienia wykonają poszczególni, wspólnie ubiegający się o udzielenie zamówienia*, Wykonawcy:

1. Wykonawca (nazwa): .....

   wykona: .....

2. Wykonawca (nazwa): .....

   wykona: .....

** - dotyczy jedynie Wykonawców wspólnie ubiegających się o udzielenie zamówienia – należy dostosować formularz do liczby Wykonawców występujących wspólnie*

Uwaga:
Oświadczenie składa tylko wykonawca wspólnie ubiegający się o udzielenie zamówienia.

Należy podpisać *zgodnie z Rozporządzeniem 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.*

Sfinansowano w ramach reakcji Unii na pandemię COVID-19

Załącznik nr 5 do SWZ

ZOBOWIĄZANIE
do oddania Wykonawcy do dyspozycji niezbędnych zasobów oraz oświadczenie podmiotu udostępniającego zasoby o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu

Nazwa podmiotu udostępniającego zasoby ……,
adres: …… województwo ……
REGON: …… NIP …… e-mail ……,
nr telefonu ……
Reprezentowany przez:

……
(imię, nazwisko)

……
(podstawa do reprezentacji podmiotu udostępniającego zasoby)

na podstawie art. 118 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2023 r. poz. 1605) zobowiązuję się do udostępnienia do dyspozycji Wykonawcy:

……
(nazwa Wykonawcy)

zasobów wskazanych w niniejszym oświadczeniu na potrzeby realizacji zamówienia pod nazwą: **„Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, systemu centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami"**
Ponadto oświadczam, że:

a) udostępniam Wykonawcy zasoby, w następującym zakresie:
……
należy dokładnie wskazać, co jest przedmiotem udostępnienia (np. doświadczenie w wykonaniu dostaw, dysponowanie osobami)

b) sposób wykorzystania udostępnionych przeze mnie zasobów będzie następujący:……
należy wskazać w jaki sposób zasoby będą udostępnione i wykorzystane przy realizacji zamówienia oraz wskazać rodzaj stosunku prawnego, jaki będzie łączył wykonawcę z podmiotem udostępniającym zasoby (np. umowa o współpracy w przypadku udostępniania osób, podwykonawstwo w przypadku udostępniania doświadczenia)

c) okres wykorzystania udostępnionych przeze mnie zasobów będzie wynosił:……

d) zrealizuję następujący zakres zamówienia:……
należy wskazać jakie dostawy zrealizuje podmiot udostępniający zasoby oraz w jakim zakresie

e) w stosunku do podmiotu, który reprezentuję nie zachodzą podstawy wykluczenia z postępowania w sytuacjach określonych w SWZ

f) podmiot, który reprezentuję spełnia warunki udziału w postępowaniu, w zakresie w jakim Wykonawca powołuje się na jego zasoby.

Zobowiązanie podpisuje Podmiot udostępniający zasoby (osoby uprawnione do reprezentacji podmiotu udostępniającego zasoby):

Należy podpisać *zgodnie z Rozporządzeniem 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.*

Załącznik nr 6 SWZ/ nr 1 do umowy

OPIS PRZEDMIOTU ZAMÓWIENIA

Wykaz oferowanego sprzętu wraz ze wskazaniem w tym wykazie oznaczeń identyfikujących oferowany przedmiot zamówienia *(należy podać oferowane parametry – pod rygorem odrzucenia oferty);*

Wymagania ogólne

W celu poprawnej integracji wszystkie oferowane rozwiązania muszą pochodzić od jednego producenta.

System bezpieczeństwa (UTM) – 2 sztuki

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie usług dostarczanych od dostawcy łącza internetowego.

Wymagania minimalne	**Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.)**
Należy podać producenta i oferowany model	
System realizujący funkcję Firewall musi zapewnić pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.	
System musi umożliwić budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.	
System musi wspierać protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego	
Redundancja, monitoring i wykrywanie awarii	
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall musi zapewnić funkcję synchronizacji sesji.	
System musi zapewnić monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.	
System musi umożliwić monitoring stanu realizowanych połączeń VPN.	
System musi umożliwić agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje	

możliwość tworzenia interfejsów redundantnych.	
Interfejsy, Dysk, Zasilanie	
System musi dysponować co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portów Gigabit Ethernet RJ-45.	
System musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 4G/5G oraz instalacji oprogramowania z klucza USB.	
System realizujący funkcję firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności 128 GB.	
System musi umożliwić skonfigurowanie co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.	
System musi być wyposażony w zasilanie AC wraz z zasilaczem.	
Parametry wydajnościowe	
W zakresie Firewall'a musi obsługiwać nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.	
Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.	
Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.	
Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 - 1.3 Gbps.	
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - 650 Mbps.	
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – 600 Mbps.	
Funkcje Systemu Bezpieczeństwa	
W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje:	
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.	
Kontrola Aplikacji.	
Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.	
Ochrona przed malware.	
Ochrona przed atakami - Intrusion Prevention System.	
Kontrola dostępu do stron WWW.	
Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.	

Zarządzanie pasmem (QoS, Traffic shaping).	
Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).	
Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Zamawiający dysponuje urządzeniami mobilnymi na których zainstalowano system Android w wersji 11. Wsparcie dla tokenów programowych (software token) musi być realizowane dla co najmniej takiego systemu operacyjnego oraz wyższych wersji systemu Android w przypadku ich aktualizacji (do najnowszej dostępnej wersji w dniu dostawy). Dla tokenów na system Android wymaga się: aktywacji z centralnego systemu uwierzytelniania (seed provisioning), możliwości konfiguracji ilości generowanych cyfr (6 lub 8), generowania kodu (cyfr) co 30 lub 60 sekund, możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ochrony dostępu poprzez konfigurowalny kod PIN.	
Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.	
Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.	
Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).	
Polityki, Firewall	
W ramach polityk i firewalla muszą być realizowane wszystkie poniższe funkcje:	
Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.	
System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.	
W ramach systemu możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.	

System wykorzystuje w politykach bezpieczeństwa zewnętrzne repozytoria zawierających: kategorie URL, adresy IP.	
Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.	
System posiada możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.	
Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX.	
Połączenia VPN	
W ramach połączeń VPN muszą być realizowane wszystkie poniższe funkcje:	
System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewnić: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • 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. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site.	

System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewnić: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.	
Routing i obsługa łączy WAN	
W zakresie routingu rozwiązanie musi zapewnić obsługę:	
Routingu statycznego.	
Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).	
Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.	
Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.	
ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.	
BFD (Bidirectional Forwarding Detection).	
Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.	
Funkcje SD-WAN	
System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.	
SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).	
Zarządzanie pasmem	
System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	
System daje możliwość określania pasma dla poszczególnych aplikacji.	
System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.	
System zapewnia możliwość zarządzania pasmem	

dla wybranych kategorii URL.	
Ochrona przed malware	
W ramach systemu ochrony przez malware muszą być realizowane wszystkie poniższe funkcje:	
Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	
Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.	
System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.	
System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.	
System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego).	
Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	
System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.	
System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	
Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.	
Ochrona przed atakami	
W ramach systemu ochrony przed atakami muszą być realizowane wszystkie poniższe funkcje:	
Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	
System chroni przed atakami na aplikacje pracujące na niestandardowych portach.	
Baza sygnatur ataków zawiera minimum 5000	

wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	
Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.	
System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	
System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.	
Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).	
Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.	
Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.	
Kontrola aplikacji	
W ramach kontroli aplikacji muszą być realizowane wszystkie poniższe funkcje:	
Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	
Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	
Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	
Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	
Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.	
Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).	
System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).	
Kontrola WWW	
W ramach kontroli WWW muszą być realizowane wszystkie poniższe funkcje:	
Moduł kontroli WWW korzysta z bazy zawierającej	

co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	
W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	
Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.	
Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	
Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).	
Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.	
Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.	
Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.	
System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.	
Uwierzytelnianie użytkowników w ramach sesji	
W ramach uwierzytelnianie użytkowników w ramach sesji muszą być realizowane poniższe funkcje:	
System Firewall umożliwia 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.	
System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.	
System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.	
Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.	

Zarządzanie	
W ramach systemu zarządzania muszą być realizowane wszystkie poniższe funkcje:	
Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.	
Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.	
Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	
System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.	
System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	
Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	
Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	
Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).	
Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.	
Logowanie	
W ramach systemu logowania muszą być realizowane wszystkie poniższe funkcje:	
Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.	
W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.	

Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.	
Możliwość włączenia / wyłączenia logowania per reguła w polityce firewall.	
System zapewnia możliwość logowania do serwera SYSLOG.	
Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.	
Testy wydajnościowe oraz funkcjonalne	
Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy wydajnościowe.	
Serwisy i licencje	
Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android w wersji 11 będącym na wyposażeniu zamawiającego), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.	
Gwarancja oraz wsparcie	
Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

Rozszerzone wsparcie serwisowe AHB/SOS	
System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres co najmniej 60 miesięcy. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001:2015 lub równoważny w zakresie świadczenia usług serwisowych – dokumenty potwierdzające należy załączyć do oferty. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym. Wymagania powinny być potwierdzone dokumentem oświadczanie wykonawcy lub producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) dołączyć do oferty.	

Wymagania ogólne

W celu poprawnej integracji wszystkie oferowane rozwiązania muszą pochodzić od jednego producenta (z wyłączeniem serwera do instalacji oprogramowania). Zamawiający aktualnie dysponuje 20 urządzeniami Fortigate-60F i oferowany systemu musi umożliwiać pełną współpracę oraz pełną integrację, ze wskazanymi urządzeniami.

System centralnego logowania – 1 sztuk

Wymagania minimalne	Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.)
A. System centralnego logowania	
Wymagania ogólne	
Należy podać producenta i model oferowanego rozwiązania	
W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w	

ramach całej infrastruktury zabezpieczeń	
Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: Microsoft Hyper-V Server 2010, 2012 R2, 2016, 2022; VMware ESXi, ESX wersje:4,5,6; Xen, Microsoft Azure.	
Interfejsy, Dysk	
System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.	
Parametry wydajnościowe	
System musi być w stanie przyjmować minimum 10 GB logów na dzień.	
Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.	
Logowanie	
Podgląd logowanych zdarzeń w czasie rzeczywistym.	
Możliwość przeglądania logów historycznych z funkcją filtrowania.	
System musi oferować 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. Muszą one obejmować co najmniej: • Listę najczęściej wykrywanych ataków. • Listę najbardziej aktywnych użytkowników. • Listę najczęściej wykorzystywanych aplikacji. • Listę najczęściej odwiedzanych stron www. • Listę krajów, do których nawiązywane są połączenia. • Listę najczęściej wykorzystywanych polityk Firewall. • Informacje o realizowanych połączeniach IPSec.	
Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie 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.	

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.	
Raportowanie	
W zakresie raportowania system musi zapewniać:	
Generowanie raportów co najmniej w formatach: PDF, CSV.	
Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.	
Funkcję definiowania własnych raportów.	
Możliwość spolszczenia raportów.	
Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.	
Korelacja logów	
W zakresie korelacji zdarzeń system musi zapewniać:	
Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.	
Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.	
Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.	
Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.	
Zarządzanie	
W zakresie zarządzania system musi zapewniać:	
System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli 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 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.	
Serwisy i licencje	
Wsparcie: System musi być objęty serwisem producenta przez okres co najmniej 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	
B. System uwierzytelniania, autoryzacji i kontroli dostępu	
Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje.	
Należy podać producenta i model oferowanego rozwiązania	
Parametry systemu	
Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę: • 4 wirtualnych interfejsów sieciowych. • Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server 2010, 2012 R2, 2016, 2022; VMware ESXi, ESX wersje:4,5,6; Xen, Microsoft Azure.	
Parametry wydajnościowe i licencyjne	
System musi obsługiwać co najmniej: • Uwierzytelnianie dla 100 użytkowników. • 25 tokenów dla uwierzytelniania dwuskładnikowego. • 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu). • Możliwość zdefiniowania co najmniej 10 grup użytkowników, • 5 lokalnych centrów certyfikacji (CA). • Możliwość wygenerowania 100 certyfikatów dla użytkowników.	
Wymagania ogólne	
System musi zapewniać nie mniej niż:	
Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności.	
Graficzną reprezentację statusu uwierzytelnionych użytkowników.	
Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:	

• Lokalnie. • Zdalnie w oparciu o protokół Syslog.	
Konfigurację Captive Portalu.	
Wymagania funkcjonalne – uwierzytelnianie	
Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż:	
Lokalną, wbudowaną bazę użytkowników.	
Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo.	
Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników.	
Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV.	
Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie: • poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych), • czasu ważności hasła,	
Konfigurowalną politykę blokowania kont, która będzie uwzględniać: • ilość nieudanych logowań, • czas blokowania konta, • okres nieaktywności, po którym konto jest blokowane.	
Możliwość odzyskiwania haseł: • z wykorzystaniem adresu email, • z wykorzystaniem pytania pomocniczego.	
Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować: • wbudowany serwer RADIUS, • integrację z zewnętrznymi serwerami RADIUS – praca jako klient.	
Obsługę protokołu LDAP, w tym zakresie system musi oferować: • wbudowany serwer LDAP, • możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).	
Obsługę protokołu SAML - Identity Provider (IdP) proxy.	
Realizację funkcji SSO (Single Sign On) w oparciu o: • integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny, • dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,	

• kontekst użytkownika przesyłany z serwera RADIUS, • informacje uzyskiwane poprzez protokół Syslog.	
Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe	
Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż:	
Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Zamawiający dysponuje urządzeniami mobilnymi na których zainstalowano system Android w wersji 11. Wsparcie dla tokenów programowych (software token) musi być realizowane dla co najmniej takiego systemu operacyjnego oraz wyższych wersji systemu Android w przypadku ich aktualizacji (do najnowszej dostępnej wersji w dniu dostawy). Dla tokenów na system Android wymaga się: aktywacji z centralnego systemu uwierzytelniania (seed provisioning), możliwości konfiguracji ilości generowanych cyfr (6 lub 8), generowania kodu (cyfr) co 30 lub 60 sekund, możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), ochrony dostępu poprzez konfigurowalny kod PIN.	
Zamawiający dysponuje komputerami z zainstalowanym systemem Microsoft Windows 10 / 11 w wersji PRO. Należy zapewnić możliwość integracji z logowaniem do systemu Windows.	
Wymagania funkcjonalne – 802.1x	
System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:	
Obsługa co najmniej poniższych protokołów EAP: • PEAP, • EAP-TTLS, • EAP-TLS, • EAP-GTC.	
Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication).	
Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.	
Wymagania funkcjonalne – zarządzanie certyfikatami	
System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:	
Obsługa wbudowanego CA (Certificate Authority).	
Obsługa CA pośredniczących (Intermediate CA).	

Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego.	
Możliwość pobrania wygenerowanych certyfikatów.	
Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP.	
Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP.	
Możliwość generowania certyfikatów typu wildcard.	
Realizacja CRL (Certificate Revocation List).	
Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).	
Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.	
Zarządzanie	
W zakresie zarządzania system musi zapewniać:	
Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki.	
System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS.	
Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć.	
Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.	
Serwis	
Wymaga się aby dostawa obejmowała również serwis producenta przez okres co najmniej 60 miesięcy, uprawniający do aktualizacji oprogramowania oraz wsparcia technicznego w języku polskim w trybie 24x7.	
C. Serwer do instalacji systemu centralnego logowania z systemem uwierzytelniania, autoryzacją i kontrolą dostępu	
Należy podać producenta i model oferowanego rozwiązania	
Obudowa	
Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz	

monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android w wersji 11 – będący na wyposażeniu zamawiającego) przy użyciu jednego z protokołów BLE/ WIFI.	
Płyta główna	
Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 56 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	
Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	
Procesor	
Zainstalowane dwa procesory każdy min. 12-rdzeniowy, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 216 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.	
RAM	
Minimum 128GB DDR5 RDIMM 4800MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 8TB pamięci RAM.	
Funkcjonalność pamięci RAM	
Advanced ECC, Self Healing, Memory Health Check, DIMM Map Out, Memory Page Retire, Fault Resilient Memory	
Gniazda PCI	
Minimum trzy sloty PCIe x16 (2 gniazda 5 generacji 4, 1 gniazdo 4 generacji) możliwość zmiany slotów na min. 2 sloty PCIe x16 5 generacji	
Interfejsy sieciowe/FC/SAS	
Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) W komplecie dostarczone 2 wkładki SFP+ producenta serwera Dodatkowa dwuportowa karta 32Gb FC.	
Dyski twarde	
Możliwość instalacji dysków SAS, SATA, SSD Zainstalowane 5 dysków 1.92TB SSD vSAS Mixed Use 12Gbps 512e 2.5in Hot-Plug ,AG Drive SED, 3DWPD	

Kontroler RAID	
Sprzętowy kontroler dyskowy, posiadający min. 8 GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. Wsparcie dla dysków 22.5 Gbps SAS, 12 Gbps SAS, and 6 Gbps SATA/SAS. Gen3 (8 GT/s) and Gen4 (16 GT/s) NVMe	
System operacyjny/System wirtualizacji	
Microsoft Windows Serwer Standard 2022 2 core z ubezpieczeniem wersji na okres 3 lat w licencjonowaniu Microsoft MPSA – 24 sztuki lub równoważny spełniający min. poniższe wymagania: • Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i czterech wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. • Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.	

• Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). • Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2019/2016.	
Wbudowane porty	
4 x USB z czego nie mniej niż 1x USB 3.0, 2x VGA	
Video	
Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200	
Zasilacze	
Redundantne, Hot-Plug min. 1400W każdy.	
Bezpieczeństwo	
• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.	

• Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej. Dane muszą być usunięte zgodnie ze standardem Instant Secure Erase. • BIOS musi posiadać możliwość przełączenia do trybu uniemożliwiającego zmianę jego konfiguracji oraz jakiekolwiek zmianę w firmware komponentów serwera. • Możliwość automatycznego przywrócenia BIOS do poprzedniej wersji w przypadku wykrycia nieautoryzowanej modyfikacji.	
Diagnostyka	
Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.	
Karta Zarządzania	
Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6;	

• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera bez konieczności instalacji dodatkowego oprogramowanie oraz niezależnie od zainstalowanego systemu operacyjnego • Obsługa Redfish SSE • Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android w wersji 11 – będący na wyposażeniu zamawiającego) przy użyciu jednego z protokołów BLE lub WIFI.	
Oprogramowanie do zarządzania	
• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu.	

• Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.	

• Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. • Dostarczone oprogramowanie powinno umożliwiać stworzenie niestandardowego automatycznego działania dla wykrytego zdarzenia • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Integracja oprogramowanie zarządzającego z konsolami zarządzania typu vCenter i MS System Center • Dostarczone oprogramowanie powinno umożliwiać zarządzanie urządzeniami firm trzecich bez potrzeby instalacji dedykowanego oprogramowania. • Umożliwia aktualizację firmware i sterowników komponentów serwera • Obsługa do minimum 8000 urządzeń per instancja	
Certyfikaty	
Serwer musi być wyprodukowany zgodnie z normami ISO-9001:2015, ISO-50001 oraz ISO-14001 lub normami równoważnymi. Serwer musi posiadać deklarację zgodności CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność	

sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca dołączy do oferty dokument potwierdzający spełnianie wymogu. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. Zaoferowane w urządzeniu zasilacze muszą posiadać wydajność na poziomie Titanium. Do Oferty należy dostarczyć wydruk ze strony 80plus.org potwierdzający spełnienie wymogu. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera (wg wytycznych Krajowej Agencji Poszanowania Energii S.A, zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 lub równoważną dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr - Wykonawca złoży dokument potwierdzający spełnianie wymogu.	
Dokumentacja użytkownika	
Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	
Gwarancja oraz wsparcie	
60 miesięcy gwarancji producenta. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem dedykowanej do tego celu aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Technik Wykonawcy lub Producenta z właściwym zestawem części do	

naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie Zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia lub zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego do wyznaczonego Kierownika Eskalacji po stronie Wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego zaoferowanego rozwiązania, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających co najmniej: wykrywanie usterek sprzętowych z predykcją awarii oraz automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji u Producenta zaoferowanego rozwiązania do co najmniej 84 miesięcy. Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący musi posiadać ISO 9001:2015 lub równoważny oraz ISO-27001 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzację producenta zaoferowanych urządzeń do wykonywania napraw – dokumenty potwierdzające należy załączyć do	

oferty. Wymagane dołączenie do oferty oświadczenia Wykonawcy lub Producenta potwierdzające, że serwis urządzeń będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym producenta za pośrednictwem wykonawcy.	

System centralnego zarządzania urządzeniami bezpieczeństwa oraz logowania – 1 sztuka

W ramach postępowania wymaganym jest dostarczenie systemu centralnego zarządzania oraz logowania i raportowania, przystosowanego do współpracy z systemem bezpieczeństwa sieciowego Fortigate 60-F będącym na wyposażeniu zamawiającego. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej.

Wymagania minimalne	Parametry oferowane (należy podać oferowane parametry, nie dopuszcza się stwierdzeń TAK, OK itp.)
Należy podać producenta i oferowany model	
Interfejsy, Dyski	
System musi dysponować co najmniej: • 4 portami Gigabit Ethernet RJ-45, • oraz portem konsoli szeregowej.	
Powierzchnia dyskowa min. 8 TB.	
Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0,1	
System musi być wyposażony w zasilanie AC.	
Parametry wydajnościowe	
System musi umożliwiać zarządzenie co najmniej 40 systemami bezpieczeństwa Fortigate 60-F lub wyższymi.	
Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 40 systemów Fortigate 60-F lub wyższymi.	
System musi być w stanie przyjmować minimum 2 GB logów na dzień.	
Funkcje systemu centralnego zarządzania	
W ramach centralnego systemu zarządzenia muszą być realizowane co najmniej poniższe funkcje:	
System musi posiadać system zarządzenia zmianami konfiguracji (WorkFlow, mechanizm audytu oraz porównania konfiguracji).	
System musi dawać możliwość pełnej konfiguracji urządzeń, ze wszystkimi ich funkcjami	

składowymi.	
System musi posiadać możliwość skonfigurowania godziny implementacji zmian (harmonogram dla instalowania zmian).	
System musi przechowywać i implementować polityki bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.	
System musi wersjonować polityki w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.	
System musi umożliwiać zarządzenie wersjami firmware'u oraz zapewniać centralną aktualizację oprogramowania.	
System musi być w stanie wysłać tą samą konfigurację na wiele urządzeń.	
System musi umożliwiać pracę wielu administratorów jednocześnie (system musi mieć możliwość blokady kontekstu urządzenia).	
System musi być w stanie zarządzać wersjami baz sygnatur na urządzeniach oraz zdalnymi uaktualnieniami.	
System musi zapisywać i zdalne wykonywanie skryptów na urządzeniach.	
System musi monitorować w czasie rzeczywistym stan urządzeń (użycie CPU, RAM).	
System musi automatyzować proces konfiguracji struktur VPN typu hub-and-spoke oraz full-mash.	
Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.	
Funkcje logowania	
Podgląd logowanych zdarzeń w czasie rzeczywistym.	
Możliwość przeglądania logów historycznych z funkcją filtrowania.	
System musi oferować 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. Muszą one obejmować co najmniej: • Listę najczęściej wykrywanych ataków. • Listę najbardziej aktywnych użytkowników. • Listę najczęściej wykorzystywanych aplikacji. • Listę najczęściej odwiedzanych stron www. • Listę krajów, do których nawiązywane są połączenia.	

• Listę najczęściej wykorzystywanych polityk Firewall. • Informacje o realizowanych połączeniach IPSec.	
Funkcja raportowania	
Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.	
Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.	
Funkcję definiowania własnych raportów.	
Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.	
Funkcje korelacji	
W zakresie korelacji zdarzeń system musi zapewniać:	
Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.	
Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.	
Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: • Malware. • Aplikacje sieciowe. • Email. • IPS. • Traffic. • Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.	
Zarządzanie	
System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.	
Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, TACACS+, PKI.	
System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i elementów	

zarządzania z perspektywy poszczególnych zarządzanych systemów.	
System musi posiadać API które umożliwia zarządzenie urządzeniami podłączonymi do systemu za pomocą poleceń REST API.	
Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.	
Gwarancja oraz wsparcie	
Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

Szkolenia, instalacja i konfiguracja

Należy wykonać szkolenie dla 25 pracowników Państwowej Inspekcji Sanitarnej z województwa zachodniopomorskiego (wskazanych przez zamawiającego) z obsługi urządzeń Fortigate 60F wyposażonymi w system operacyjny FortiOS w wersji 7.4.1. Szkolenie musi być przeprowadzone przez osobę / osoby legitymujące się certyfikatem na poziomie NSE8 (zamawiający może zażądać numerów certyfikatów, które muszą być weryfikowalne poprzez wprowadzenie ich na dedykowanej stronie internetowej producenta dostępnej (na dzień publikacji ogłoszenia) pod adresem: https://training.fortinet.com/mod/customcert/verify_certificate.php). Szkolenie może obywać się zdalnie w grupach maksymalnie 10 osobowych. Długość szkolenia dla każdej grupy wynosi 3 dni robocze. Szkolenie musi być realizowane w języku polskim. Szkolenie musi zostać realizowane w ciągu 3 miesięcy od daty dostawy a termin szkolenia zostanie ustalony w porozumieniu z Wykonawcą.

W ramach dostawy należy wykonać także szkolenie dla 5 pracowników Państwowej Inspekcji Sanitarnej z województwa zachodniopomorskiego (wskazanych przez zamawiającego) z oferowanej technologii systemu centralnego zarządzania, systemów centralnego logowania z systemem uwierzytelniania, autoryzacją i kontrolą dostępu. Szkolenie musi być przeprowadzone przez certyfikowanego w zakresie cyberbezpieczeństwa inżyniera oferowanej technologii. Poziom certyfikacji musi być na najwyższym poziomie dostępnym u producenta oferowanej technologii (zamawiający może zażądać numerów certyfikatów, które muszą być weryfikowalne poprzez wprowadzenie ich na dedykowanej stronie internetowej producenta zaproponowanego rozwiązania). Szkolenie może odbyć się zdalnie. Długość szkolenia wynosi 3 dni robocze. Szkolenie musi być realizowane w języku polskim. Szkolenie musi zostać realizowane w ciągu 3 miesięcy od daty dostawy a termin szkolenia zostanie ustalony w porozumieniu z Wykonawcą.

Wykonawca musi zapewnić wsparcie wdrożeniowe obejmujące całość zamówienia dla zamawiającego w wymiarze 80 godzin roboczych. Wsparcie musi być udzielone przez minimum dwóch inżynierów posiadających certyfikaty oferowanej technologii. Poziom certyfikacji musi być na najwyższym poziomie dostępnym u producenta oferowanej technologii (zamawiający może zażądać numerów certyfikatów, które muszą być weryfikowalne poprzez wprowadzenie ich na dedykowanej stronie internetowej producenta zaproponowanego rozwiązania). W przypadku gdy wsparcie zostanie udzielone przez producenta zaproponowanego rozwiązania a wsparcie będzie realizowane przez dużą grupę pracowników certyfikaty nie są wymagane. Całość procesu wsparcia musi być realizowana w języku polskim. Do kontaktu z inżynierami wyznaczeni zostaną pracownicy Państwowej Inspekcji Sanitarnej wskazani przez zamawiającego.

Załącznik nr 7 do SWZ

UMOWA Nr .....

zawarta w dniu .....2023 r. w..... pomiędzy:
Skarbem Państwa - ..... w ....., ul. ....., ..., NIP ....., REGON: ....., zwanym w dalszej treści niniejszej umowy „Zamawiającym",
którego reprezentuje:

1) ..... .
2) .....

a
....., NIP ....., REGON ....., KRS..... ,
zwanym w dalszej treści niniejszej umowy "Wykonawcą"
którego reprezentuje:

§1

Niniejsza umowa zostaje zawarta w wyniku dokonania przez Zamawiającego wyboru oferty Wykonawcy, w postępowaniu publicznym, pn. **„Dostawa systemu bezpieczeństwa (UTM), centralnego systemu logowania, systemu centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami",** prowadzonym na podstawie art. 275 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych.

§2

1. Przedmiotem zamówienia jest dostawa systemu bezpieczeństwa (UTM) – 2 szt., centralnego systemu logowania, systemu centralnego zarządzania urządzeniami bezpieczeństwa wraz ze szkoleniami.
2. Szczegółowy opis przedmiotu zamówienia (OPZ) zawarty jest w **załączniku nr 1** do umowy.
3. Wykonawca oświadcza, że przedmiot umowy określony w ust. 1 spełnia wymagania określone w OPZ i jest zgodny z ofertą Wykonawcy stanowiącą **załącznik nr 2** do umowy.
4. Wykonawca oświadcza, że przedmiot umowy jest fabrycznie nowy, nie poleasingowy, nieużywany oraz nieeksponowany na wystawach, pochodzi z autoryzowanego źródła sprzedaży, sprawny technicznie, wolny od wad prawnych i fizycznych, bezpieczny, kompletny i gotowy do pracy, a także spełnia wymagania techniczno-funkcjonalne wyszczególnione w szczegółowym OPZ.
5. Wykonawca oświadcza, że przedmiot umowy określony w ust. 1 jest dopuszczony do obrotu prawnego na terytorium RP.
6. Oferowany przedmiot zamówienia spełnia wszelkie wymogi norm określonych obowiązującym prawem.
7. Zamawiający i Wykonawca, wybrany w postępowaniu o udzielenie zamówienia, zobowiązani są współdziałać przy wykonaniu umowy w sprawie zamówienia publicznego, w celu należytej realizacji zamówienia.
8. Przed podpisaniem protokołu odbioru Wykonawca przekaże Zamawiającemu komplet dokumentów w języku polskim/ angielskim, w szczególności:
   1) karty gwarancyjne,
   2) instrukcje obsługi i dokumentację techniczną oferowanego sprzętu,
   3) dokumenty określające zasady świadczenia usług przez autoryzowany serwis w okresie gwarancyjnym,
   4) licencje jak również wszelkie prawa na dostarczone programy i systemy operacyjne, wystawione na rzecz Zamawiającego,
   5) certyfikaty/ równoważne dokumenty dla minimum dwóch inżynierów zgodnie z OPZ.
9. Przedmiot zamówienia jest współfinansowany na podstawie realizacji projektu „Wzmocnienie infrastruktury powiatowych stacji sanitarno-epidemiologicznych w celu zwiększenia efektywności ich działania" realizowanego w ramach osi priorytetowej XI REACT-EU działania 11.3 Wspieranie naprawy i odporności systemu ochrony zdrowia Programu Operacyjnego Infrastruktura i Środowisko na lata 2014-2020 w

zakresie wsparcia organów Państwowej Inspekcji Sanitarnej, opartego na porozumieniu zawartym pomiędzy Głównym Inspektoratem Sanitarnym a każdą z Powiatowych Stacji Sanitarno-Epidemiologicznych będących Zamawiającym.

§3

1. Wykonawca zobowiązuje się zrealizować przedmiot umowy na podstawie niniejszej umowy.
2. Termin dostawy przedmiotu umowy- **do 14 dni od dnia zawarcia umowy.**
3. Jeżeli zwłoka, w stosunku do terminu określonego w ust. 2, przekroczy **3 dni robocze,** Zamawiający zastrzega sobie prawo odstąpienia od Umowy z winy Wykonawcy.
4. Przedmiot umowy Wykonawca dostarczy na własny koszt i ryzyko do Powiatowej Stacji Sanitarno-Epidemiologicznej w Szczecinku, ul. Ordona 22, 78-400 Szczecinek.
5. Transport przedmiotu zamówienia krajowy i zagraniczny wraz z ubezpieczeniem, wszelkimi opłatami celnymi, skarbowymi oraz innymi opłatami pośrednimi obciążają Wykonawcę.
6. Wykonawca zobowiązuje się, co najmniej na **3 dni** przed planowanym terminem dostawy, powiadomić Zamawiającego drogą elektroniczną na adres poczty elektronicznej: ..... o dacie i godzinie dostawy.
7. Odbiór będzie polegał na stwierdzeniu zgodności z OPZ oraz Ofertą Wykonawcy, w szczególności braku uszkodzeń mechanicznych, pochodzenia z autoryzowanego źródła czy poprawności działania. Z czynności odbioru zostanie sporządzony protokół odbioru Przedmiotu Umowy. Protokół winien dodatkowo zawierać wszelkie uwagi i zastrzeżenia, w tym w zakresie pochodzenia przedmiotu umowy z autoryzowanego źródła.
8. W przypadku stwierdzenia wad lub niezgodności Przedmiotu Umowy z treścią OPZ lub Ofertą Wykonawcy lub postanowieniami niniejszej umowy, w szczególności stwierdzenia uszkodzeń mechanicznych, niezgodności w zakresie parametrów technicznych jak i funkcjonalnych, pochodzenia przedmiotu umowy z nie autoryzowanego źródła Wykonawca niezwłocznie, ale nie później niż w terminie **7 dni,** dokona wymiany przedmiotu umowy na wolny od stwierdzonych wad lub niezgodności z treścią z OPZ. Nie dokonanie wymiany, w powyższym terminie, skutkuje uprawnieniem Zamawiającego do odstąpienia od umowy z winy Wykonawcy.
9. Szkolenia, o których mowa w załączniku nr 1 do umowy, będą odbywać się w terminach uzgodnionych przez Strony, w okresie eksploatacji przedmiotu umowy.
10. Do koordynacji spraw związanych z przedmiotem zamówienia Wykonawca upoważnia .....tel. ....., e-mail: .....
11. Do koordynacji spraw związanych z przedmiotem zamówienia Zamawiający upoważnia ..... tel..... e-mail: .....

§4

1. Za prawidłowe wykonanie Przedmiotu umowy, Zamawiający zapłaci Wykonawcy **cenę brutto** ..... **złotych** (słownie) ....., w tym podatek VAT 23%.
2. Wynagrodzenie Wykonawcy obejmuje wszystkie elementy przedmiotu zamówienia wymienione w OPZ.
3. Rozliczenie nastąpi w formie przelewu, z konta Zamawiającego na konto Wykonawcy, w terminie do 30 dni kalendarzowych, licząc od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury. Termin, o którym mowa w zdaniu pierwszym jest zastrzeżony na korzyść Zamawiającego. Podanie na fakturze terminu płatności innego niż w zdaniu powyżej nie zmienia warunków płatności.
4. Podstawą wystawienia faktury przez Wykonawcę jest podpisany przez Zamawiającego bez zastrzeżeń protokół odbioru, o którym mowa w§ 3 ust. 7 Umowy.
5. Za datę dokonania przez Zamawiającego płatności uznaje się datę złożenia przelewu należności w banku Zamawiającego.
6. Jeśli numer rachunku rozliczeniowego wskazany przez Wykonawcę jest rachunkiem, dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. - *Prawo Bankowe* prowadzony jest rachunek VAT to:
   1) Zamawiający oświadcza, że będzie realizować płatności za faktury z zastosowaniem mechanizmu podzielonej płatności tzw. ,,split payment". Zapłatę w tym systemie uznaje się za dokonanie płatności w terminie ustalonym w ust. 3,
   2) Podzieloną płatność tzw. ,,split payment" stosuje się wyłącznie przy płatnościach bezgotówkowych, realizowanych za pośrednictwem polecenia przelewu lub polecenia zapłaty dla czynnych podatników VAT. Mechanizm podzielonej płatności nie będzie wykorzystywany do zapłaty za czynności lub zdarzenia pozostające poza zakresem VAT (np. zapłata kar, odszkodowania), a także za świadczenia zwolnione z VAT, opodatkowane stawką 0% lub objęte odwrotnym obciążeniem,

3) Wykonawca oświadcza, że wyraża zgodę na dokonywanie przez Zamawiającego płatności w systemie podzielonej płatności tzw. ,,split payment".

§5

1. Na przedmiot umowy Wykonawca udziela .....**miesięcznej gwarancji*.**
   *) ***zgodnie z ofertą Wykonawcy- kryterium oceny ofert***
2. Okres rękojmi jest tożsamy z okresem gwarancji.
3. Termin udzielonej gwarancji i rękojmi rozpoczyna bieg od momentu aktywacji licencji na urządzeniu, o którym mowa w§ 2 ust. 1.
4. Wykonawca, w okresie gwarancji, gwarantuje czas reakcji serwisu zgodnie z wymaganiami określonymi w OPZ.
5. Okres trwania gwarancji i rękojmi będzie automatycznie wydłużony, od dnia zgłoszenia wady lub nieprawidłowości działania urządzenia, do czasu faktycznego jego naprawienia i udostępnienia go Zamawiającemu.
6. Wszelkie koszty związane ze świadczeniem usług gwarancyjnych obciążają Wykonawcę.
7. W razie nieuwzględnienia reklamacji przez Wykonawcę, Zamawiający może wystąpić z wnioskiem o przeprowadzenie ekspertyzy przez rzeczoznawcę z danej dziedziny.
8. Jeżeli reklamacja Zamawiającego okaże się uzasadniona, koszty związane z przeprowadzeniem ekspertyzy oraz koszty związane z usunięciem wad ponosi Wykonawca.
9. Jeżeli w okresie gwarancji, na skutek dostarczenia przez Wykonawcę wadliwego przedmiotu umowy Zamawiający poniesie dodatkowe koszty, związane z wykonywaną w oparciu o wadliwy przedmiot umowy działalnością, Wykonawca zobowiązuje się do zwrotu Zamawiającemu tych kosztów, po uprzednim uzgodnieniu formy zwrotu.
10. Zamawiający ma prawo dochodzić uprawnień przysługujących z tytułu rękojmi za wady, niezależnie od uprawnień wynikających z gwarancji.
11. W przypadku stwierdzenia usterki/wady przedmiotu umowy w okresie objętym gwarancją, Strony komunikują się za pośrednictwem poczty elektronicznej. Korespondencję w powyższym zakresie kierować należy na adres mailowy:
    1) Zamawiającego - .....
    2) Wykonawcy - .....
12. Wykonawca zapewni autoryzowany polskojęzyczny serwis gwarancyjny.

§6

1. Zamawiający ma prawo naliczyć Wykonawcy karę umowną w następujących okolicznościach:
   1) w przypadku odstąpienia od umowy przez Wykonawcę lub Zamawiającego, z przyczyn zawinionych po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości **10%** wartości wynagrodzenia brutto, o którym mowa w§ 4 ust. 1 umowy;
   2) w przypadku zwłoki w realizacji przedmiotu umowy, w terminie określonym w § 3 ust. 2 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości **1%** wartości wynagrodzenia brutto, o którym mowa w§ 4 ust. 1 umowy, za każdy dzień zwłoki;
   3) w przypadku zwłoki w wymianie sprzętu na wolny od wad/na wolny od niezgodności lub naprawie wadliwego przedmiotu umowy, w terminie określonym w § 3 ust. 8 lub § 5 ust. 4 umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości **0,5** % wartości wynagrodzenia brutto, o którym mowa w§ 4 ust. 1 umowy za każdy dzień zwłoki.
2. Limit kar umownych, z tytułów przewidzianych w niniejszej umowie, wynosi **25** % wartości wynagrodzenia brutto określonego w§ 4 ust. 1.
3. Kary umowne stają się wymagalne w pierwszym dniu kiedy możliwe jest ich naliczenie, a w przypadku kar za zwłokę z każdym dniem zwłoki.
4. Zamawiający może dochodzić odszkodowania uzupełniającego przenoszącego wysokość kar umownych na zasadach ogólnych kodeksu cywilnego.
5. Zamawiającemu przysługuje prawo potrącenia kar umownych z wynagrodzenia Wykonawcy. Wysokość oraz rodzaj nałożonej kary zostaną określone przez Zamawiającego w nocie obciążeniowej, którą otrzyma Wykonawca.

§7

1. Zamawiającemu przysługuje w szczególności prawo odstąpienia od umowy w następujących sytuacjach:
   1) w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy w całości lub w jej części nie leży w interesie publicznym, czego nie można było przewidzieć w chwili jej zawarcia

lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. W takiej sytuacji Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy,

2) dostawy innego przedmiotu umowy niż określony w opisie przedmiotu zamówienia,
3) jeżeli Wykonawca, w chwili złożenia oferty, podlegał wykluczeniu na podstawie okoliczności, o których mowa w art. 7 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego i złożył w tym zakresie nieprawdziwe oświadczenie,
4) jeżeli Wykonawca nie dokonał wymiany sprzętu, zgodnie z wymogiem zawartym w§ 3 ust. 8 umowy,
5) jeżeli Wykonawca nie zapewni polskojęzycznego serwisu gwarancyjnego,
6) jeżeli Wykonawca nie zapewni, minimum dwóch inżynierów, posiadających certyfikaty / równoważne dokumenty, zgodnie z wymaganiami określonymi w OPZ.

2. Zamawiający będzie mógł odstąpić od umowy w każdym momencie, od powzięcia wiadomości o okolicznościach stanowiących podstawę odstąpienia.
3. Odstąpienie od niniejszej umowy uznaje się za skuteczne z chwilą doręczenia Wykonawcy oświadczenia Zamawiającego drogą mailową, na adres ....., jeśli zostanie potwierdzone następnie listem poleconym wysłanym na adres Wykonawcy.
4. Każda ze Stron może wypowiedzieć lub odstąpić od Umowy w razie zaistnienia przypadku siły wyższej, którego skutkiem jest niemożność wykonania obowiązków wynikających z Umowy przez którąkolwiek ze Stron przez okres ponad 30 dni. Po upływie wskazanego terminu każda ze Stron może wypowiedzieć lub odstąpić od Umowy ze skutkiem natychmiastowym i w drodze pisemnego oświadczenia przesłanego drugiej Stronie wraz z udowodnieniem tych okoliczności poprzez przedstawienie dokumentacji potwierdzającej wystąpienie zdarzeń mających cechy Siły wyższej oraz wskazania wpływu, jaki zdarzenie miało na przebieg realizacji umowy.
5. Przez pojęcie siły wyższej należy rozumieć zdarzenie zewnętrzne, którego nie można było przewidzieć, analizując i uwzględniając wszystkie okoliczności sprawy, jak również, któremu nie można było zapobiec znanymi, normalnie stosowanymi sposobami w szczególności zdarzenia o charakterze katastrofalnych działań przyrody albo nadzwyczajnych i zewnętrznych wydarzeń, którym zapobiec nie można, jak wojna, konflikt zbrojny na terenach graniczących z Rzecząpospolitą Polską, restrykcje stanu wojennego, powstanie, rewolucja, zamieszki.

§8

1. Przewiduje się możliwości zmiany umowy, gdy:
   1) ulegnie zmianie stan prawny w zakresie dotyczącym realizowanej umowy, który spowoduje konieczność zmiany sposobu wykonania zamówienia przez Wykonawcę;
   2) wystąpią przeszkody o obiektywnym charakterze (zdarzenia nadzwyczajne, zewnętrzne i niemożliwe do zapobieżenia, a więc mieszczące się w zakresie pojęciowym tzw. ,,siły wyższej" w tym klęski żywiołowej). W takim przypadku termin realizacji przedmiotu umowy może ulec przesunięciu o czas trwania przeszkody. Strony zobowiązują się do natychmiastowego poinformowania się nawzajem o wystąpieniu ww. przeszkód;
2. Żadnej ze stron Umowy nie przysługuje roszczenie o zawarcie aneksu (obie strony muszą wyrazić zgodę na zawarcie aneksu).

§9

1. Wykonawca nie ma prawa przenoszenia praw lub obowiązków wynikających z niniejszej umowy na rzecz osób trzecich bez zgody Zamawiającego wyrażonej pod rygorem nieważności na piśmie.
2. Nieważność lub nieskuteczność któregokolwiek z postanowień Umowy nie wpływa na ważność i skuteczność pozostałych jej postanowień. Strony będą dążyły do zastąpienia nieważnego lub nieskutecznego postanowienia przez ważne i skuteczne postanowienie, które pozwoli osiągnąć w sposób jak najbardziej zbliżony taki sam lub podobny cel Umowy.
3. Ewentualne spory wynikłe z niniejszej Umowy rozstrzygane będą przez miejscowo właściwy Sąd dla siedziby Zamawiającego.
4. Wszelka korespondencja kierowana będzie przez strony wzajemnie na adresy wskazane w nagłówku umowy. Każda ze stron zobowiązana jest niezwłocznie powiadomić drugą stronę o zmianie adresu do doręczeń wskazanego w nagłówku umowy lub pozostałych danych kontaktowych, pod rygorem uznania za

prawidłowe doręczenia na dotychczasowy adres.

5. Strony zobowiązują się do wzajemnego, niezwłocznego informowania o każdej zmianie statusu prawnego i adresu siedziby. W przypadku niedopełnienia ww. obowiązków przez którąkolwiek ze Stron, Stronę tę obciążać będą ewentualne koszty mogące wyniknąć wskutek zaniechania.
6. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu cywilnego.
7. Umowa została sporządzona w formie elektronicznej zgodnie z art. 78^1 § 1 Kodeksu cywilnego pod rygorem nieważności i zawarta w dacie złożenia podpisu przez ostatnią ze Stron.

Załączniki do umowy:

1. *Opis przedmiotu zamówienia z parametrami oferowanymi przez Wykonawcę*
2. *Oferta Wykonawcy*

…… ……

Zamawiający Wykonawca