Nr sprawy: ZP/1/IV/2018

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA (SIWZ) po zmianach z dnia 6.06.2018 r.

przetarg nieograniczony na:

„Dzierżawa systemu wirtualizacji serwerów"

Zatwierdził:

Z up. Dyrektora

Z-ca DYREKTORA
ds. Administracyjnych/Główny Księgowy
Lotnicze Pogotowie Ratunkowe

Paweł Kamiński

§ 1
NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

1. Zamawiającym jest:
   Lotnicze Pogotowie Ratunkowe
   Adres: ul. Księżycowa 5 01-934 Warszawa
   Tel: +48 /22/ 22 99 931, Fax: +48 /22/ 22 99 933
   NIP: 522-25-48-391 Regon: 016321074
   http://www.lpr.com.pl e-mail://**dzp@lpr.com.pl**, centrala@lpr.com.pl
2. Dni i godziny urzędowania: od poniedziałku do piątku w godzinach 8^{00}-15^{35}.

§ 2
TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie **przetargu nieograniczonego** na podstawie ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 z późn. zm.), zwanej dalej uPzp.
2. Postępowanie prowadzone jest zgodnie z przepisami uPzp dla postępowań, których wartość zamówienia nie przekracza kwot określonych na podstawie art. 11 ust. 8 uPzp tj. kwotę 144 000,00 EURO.

§ 3
OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dzierżawa systemu wirtualizacji serwerów dla Lotniczego Pogotowia Ratunkowego w Warszawie.
2. Szczegółowy opis przedmiotu zamówienia znajduje się w załączniku nr 2 do SIWZ stanowiącym Opis przedmiotu zamówienia.
3. Oznaczenie wg Wspólnego Słownika Zamówień (CPV):
   30230000-0 Sprzęt związany z komputerami
   30233141-1 Nadmiarowa macierz niezależnych dysków (RAID)
   32420000-3 Urządzenia sieciowe
4. W przypadku, gdyby w opisie przedmiotu zamówienia Zamawiający określił przedmiot zamówienia poprzez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, Zamawiający dopuszcza możliwość składania ofert równoważnych. Wskazane wyżej określenie przedmiotu zamówienia ma charakter wyłącznie pomocniczy w przygotowaniu oferty i ma na celu wskazać oczekiwane standardy co do minimalnych parametrów technicznych oczekiwanych materiałów i urządzeń. Przez ofertę równoważną należy rozumieć ofertę o parametrach technicznych, wytrzymałościowych, jakościowych, wydajnościowych nie gorszych od opisu wskazanego przez Zamawiającego w opisie przedmiotu zamówienia. W związku z powyższym Zamawiający dopuszcza możliwość zaoferowania materiałów o innych znakach towarowych, patentach lub pochodzeniu, natomiast nie o innych właściwościach i funkcjonalnościach niż określone w SIWZ. Wykonawca powołujący się na rozwiązania równoważne stosownie do dyspozycji art. 30 ust. 5 ustawy Pzp musi wykazać, że oferowane dostawy spełniają warunki określone przez Zamawiającego w stopniu nie gorszym. W przypadku, gdy Wykonawca nie złoży w ofercie dokumentów o zastosowaniu innych materiałów i urządzeń, to rozumie się przez to, że do kalkulacji ceny oferty oraz do wykonania umowy ujęto materiały i urządzenia zaproponowane w opisie przedmiotu zamówienia. W przypadku, gdy Zamawiający użył w opisie przedmiotu zamówienia normy, aprobaty, specyfikacje techniczne i systemy odniesienia, o których mowa w art. 30 ust. 1-3 ustawy Pzp należy rozumieć je jako przykładowe. Zamawiający zgodnie z art. 30 ust. 4 ustawy Pzp dopuszcza w każdym przypadku zastosowanie rozwiązań równoważnych opisanym w treści SIWZ. Każdorazowo, gdy wskazana jest w niniejszej SIWZ norma, należy przyjąć, że w odniesieniu do niej użyto sformułowania „lub równoważne". Wykonawca, który powołuje się na rozwiązania równoważne w stosunku do opisywanych przez Zamawiającego, jest

obowiązany wykazać w złożonej ofercie, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego.

§ 4
OPIS CZĘŚCI ZAMÓWIENIA

Zamawiający nie dopuszcza składania ofert częściowych. Oferty niezawierające pełnego zakresu przedmiotu zamówienia zostaną odrzucone.

§ 5
INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 67 UST. 1 PKT 6 I 7 UPZP

Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 7 uPzp.

§ 6
INFORMACJA O OFERTACH WARIANTOWYCH

Zamawiający nie dopuszcza składania ofert wariantowych.

§ 7
WYKONANIE ZAMÓWIENIA PRZY UDZIALE PODWYKONAWCÓW

Zgodnie z przepisem art. 36a ust. 1 uPzp Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy. Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez Wykonawcę firm podwykonawców.

W przypadku niewskazania części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i firm podwykonawców, przyjmuje się, iż przedmiot zamówienia zostanie w całości wykonany samodzielnie przez Wykonawcę.

§ 8
TERMIN WYKONANIA ZAMÓWIENIA

1. Zamawiający określa termin realizacji zamówienia na 36 miesięcy liczonych od dnia zawarcia Umowy do ostatniego dnia miesiąca, w którym nastąpi zapłata ostatniej 35 - raty dzierżawnej.
2. Szczegółowo terminy realizacji przedmiotu zamówienia określone są w § 3 załącznika nr 3 do SIWZ – Istotne Postanowienia Umowy.

§ 9
WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ PODSTAWY WYKLUCZENIA WYKONAWCY

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki, o których mowa w art. 22 ust. 1b uPzp, dotyczące:
   1) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie określa warunku ww. zakresie,
   2) sytuacji ekonomicznej lub finansowej – Zamawiający nie określa warunku ww. zakresie,
   3) zdolności technicznej lub zawodowej – o udzielenie zamówienia może się ubiegać się Wykonawca, który:
      a. w okresie ostatnich trzech (3) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał co najmniej jedno (1) zamówienie polegające na dzierżawie lub dostawie systemu wirtualizacji oraz co najmniej jedno (1) zamówienie na dzierżawę lub dostawę macierzy dyskowej wraz z serwerami, a wartość każdego wykazanego zamówienia wynosiła co najmniej 500.000,00 zł netto każde.
      b. dysponuje odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia, w tym w szczególności dedykowanym zespołem (co najmniej 1 osoba) certyfikowanych inżynierów posiadających niezbędne kompetencje związane z przedmiotem zamówienia.

2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 24 ust. 1 uPzp. Zgodnie z art. 24 ust. 1 uPzp z postępowania o udzielenie zamówienia wyklucza się:
   1) Wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie wykazał braku podstaw wykluczenia,
   2) Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      a) o którym mowa w art. 165a, art. 181–188, art. 189a, art. 218–221, art. 228–230a, art. 250a, art. 258 lub art. 270–309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. poz. 553 z późn. zm.) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2016 r. poz. 176),
      b) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny,
      c) skarbowe,
      d) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
   3) Wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2),
   4) Wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności,
   5) Wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i niedyskryminacyjne kryteria, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów,
   6) Wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia,
   7) Wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia,
   8) Wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu,
   9) Wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych,
   10) Wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz. U. z 2015 r. poz. 1212, 1844 i 1855 oraz z 2016 r. poz. 437 i 544),
   11) Wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne,
   12) Wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
3. Wykluczenie Wykonawcy następuje:

1) w przypadkach, o których mowa w ust. 2 pkt 2) lit. a) – c) i pkt 3), gdy osoba, o której mowa w tych przepisach została skazana za przestępstwo wymienione w ust. 2 pkt 1) lit. a) – c), jeżeli nie upłynęło 5 lat od dnia uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia,
2) w przypadkach, o których mowa:
   a) w ust. 2 pkt 2) lit. d) i pkt 3), gdy osoba, o której mowa w tych przepisach, została skazana za przestępstwo wymienione w ust. 2 pkt 2) lit. d),
   b) w ust. 2 pkt 4),
   – jeżeli nie upłynęły 3 lata od dnia odpowiednio uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia lub od dnia w którym decyzja potwierdzająca zaistnienie jednej z podstaw wykluczenia stała się ostateczna,
3) w przypadkach, o których mowa w ust. 2 pkt 7) i 9), jeżeli nie upłynęły 3 lata od dnia zaistnienia zdarzenia będącego podstawą wykluczenia,
4) w przypadku, o którym mowa w ust. 2 pkt 10), jeżeli nie upłynął okres, na jaki został prawomocnie orzeczony zakaz ubiegania się o zamówienia publiczne,
5) w przypadku, o którym mowa w ust. 2 pkt 11), jeżeli nie upłynął okres obowiązywania zakazu ubiegania się o zamówienia publiczne.

4. Wykonawca, który podlega wykluczeniu na podstawie ust. 2 pkt 2) i 3) oraz 5) – 9), może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Przepisu zdania pierwszego nie stosuje się, jeżeli wobec wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.
5. Wykonawca nie podlega wykluczeniu, jeżeli zamawiający, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, uzna za wystarczające dowody przedstawione na podstawie ust. 4.
6. W przypadkach, o których mowa w ust. 2 pkt 8), przed wykluczeniem Wykonawcy, Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji.
7. Zamawiający może wykluczyć wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

§ 10
WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW DO WYKLUCZENIA

1. **Wykaz oświadczeń składanych przez Wykonawcę <u>wraz z ofertą</u> w celu wstępnego potwierdzenia, że nie podlega on wykluczeniu oraz spełnia warunki udziału w postępowaniu:**
   1) Aktualne na dzień składania ofert Oświadczenie o niepodleganiu wykluczeniu składane na podstawie art. 25a ust. 1 uPzp (wzór Oświadczenia – załącznik nr 4 do SIWZ),
   2) Aktualne na dzień składania ofert Oświadczenie o spełnianiu warunków udziału składane na podstawie art. 25a ust. 1 uPzp (wzór Oświadczenia – załącznik nr 5 do SIWZ)

   oraz
   3) Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o podwykonawcach w oświadczeniu, o którym mowa w pkt 1),
   4) W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenia składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia

w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

2. Oświadczenia, o których mowa w § 10 dotyczące wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a uPzp oraz dotyczące podwykonawców, składane są w oryginale.
3. Dokumenty, o których mowa § 10, inne niż oświadczenia, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem, poprzez złożenie na każdej zapisanej stronie kopii dokumentu podpisu wraz z adnotacją „za zgodność z oryginałem".
4. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.
5. Zgodnie z art. 24 ust. 11 uPzp, Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 3 uPzp, przekaże Zamawiającemu **w formie pisemnej (bez wezwania)** oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 uPzp. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia publicznego (wzór oświadczenia stanowi załącznik nr 6 do SIWZ).
6. W zakresie nieuregulowanym w SIWZ, zastosowanie mają postanowienia Rozporządzenia Ministra Rozwoju z dnia 27 lipca 2016 roku w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia.

§ 11
INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW. WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1. W niniejszym postępowaniu komunikacja między Zamawiającym a Wykonawcami odbywa się za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830), osobiście, za pośrednictwem posłańca, faksu lub przy użyciu poczty elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z 2015 r. poz. 1844 oraz z 2016 r. poz. 147 i 615), z zastrzeżeniem ust. 2.
2. Oferty wraz z załącznikami (również ewentualną ofertę dodatkową, o której mowa w art. 91 ust. 5 uPzp) składa się pod rygorem nieważności w formie pisemnej. W przypadku oświadczeń i dokumentów składanych w trybie art. 24 ust. 11 oraz 26 ust. 1, 2, 2f uPzp oraz w przypadku oświadczeń, dokumentów i pełnomocnictw składanych odpowiednio w trybie art. 26 ust. 3 i 3a uPzp, obowiązuje forma pisemna.
3. Wykonawca może się kontaktować z Zamawiającym:
   a) numer telefonu: +48 (22) 22 99 833,
   b) numer faksu: +48 (22) 22 99 933,
   c) adres poczty elektronicznej: sekretariat@lpr.com.pl, dzp@lpr.com.pl
4. Osobą uprawnioną do kontaktów z Wykonawcami jest:
   a) w sprawach merytorycznych – Maciej Paczesny,
   b) w sprawach proceduralnych – Karolina Biela.
5. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje za pośrednictwem faksu lub przy użyciu poczty elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, każda ze Stron na żądanie drugiej Strony niezwłocznie potwierdza fakt ich otrzymania.
6. We wszelkiej korespondencji dotyczącej niniejszego postępowania zaleca się wskazywać numer postępowania i tytuł postępowania nadany przez Zamawiającego.
7. Wykonawca zobowiązany jest do poinformowania Zamawiającego o każdej zmianie adresu. Korespondencja skierowana na ostatnio podany adres Wykonawcy będzie uznana za skutecznie złożoną temu Wykonawcy.

8. Wykonawca może zwrócić się do Zamawiającego z prośbą o wyjaśnienie treści niniejszej SIWZ. Zamawiający udzieli niezwłocznie wyjaśnień jednak nie później niż na 2 dni przed terminem składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu składania wniosku, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku.

§ 12
WYMAGANIA DOTYCZĄCE WADIUM

1. Wykonawca jest zobowiązany wnieść wadium do dnia **14.06.2018** roku do **godz. 12^{30}** w wysokości **12 000,00 zł** (słownie: dwanaście tysięcy 00/100 zł).
2. Forma wpłaty wadium:
   1) Wadium może być wnoszone w:
      a) pieniądzu, płatne na konto 36 1130 1017 0020 1459 3620 0008 w banku BGK S. A.,
      b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
      c) gwarancjach bankowych,
      d) gwarancjach ubezpieczeniowych,
      e) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt. 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. Nr 109, poz. 1158 z późn. zm.).
   2) Wadium wnoszone w pieniądzu uważa się za wniesione skutecznie wówczas, gdy przed upływem terminu określonego w § 12 ust. 1 nastąpi uznanie na rachunku Zamawiającego.
   3) Wadium wnoszone w formie niepieniężnej uważa się za wniesione skutecznie wówczas, gdy przed upływem terminu określonego w § 12 ust. 1 zostanie dostarczone w oryginale do miejsca wskazanego w § 15 ust. 1. Powyższe wadium musi być dostarczone w oddzielnej trwale zamkniętej kopercie oznaczonej: „Wadium do postępowania nr **ZP/1/IV/2018** pn: **„Dzierżawa systemu wirtualizacji serwerów"**.
   4) Wszystkie dokumenty, potwierdzające wniesienie wadium muszą zawierać numer przetargu, którego dotyczą.
   5) Wadium wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy wskazany w ust. 2 pkt 1) lit. a).
   6) W przypadku składania przez Wykonawcę wadium w formie gwarancji lub poręczenia niepieniężnego, gwarancja lub poręczenie powinno być sporządzone zgodnie z obowiązującym prawem i winno zawierać następujące elementy:
      a) nazwę dającego zlecenie (Wykonawcy), beneficjenta gwarancji lub poręczenia (Zamawiającego), gwaranta (banku lub instytucji ubezpieczeniowej udzielających gwarancji lub podmiotu udzielającego poręczenia) oraz wskazanie ich siedziby, nr referencyjny nadany sprawie przez Zamawiającego, nazwę zamówienia,
      b) określenie wierzytelności, którą ma być zabezpieczona gwarancją lub poręczeniem,
      c) kwotę gwarancji lub poręczenia,
      d) termin ważności gwarancji lub poręczenia,
      e) bezwarunkowe i nieodwołalne zobowiązanie gwaranta do zapłacenia kwoty gwarancji lub poręczenia na pierwsze pisemne żądanie Zamawiającego, (nie później niż w ciągu 30 dni od daty zgłoszenia żądania), w przypadku zaistnienia okoliczności wymienionych w art. 46 ust. 4 a i art. 46 ust. 5 uPzp.
   7) Zwrot bądź zatrzymanie wadium nastąpi zgodnie z art. 46 uPzp.
3. W przypadku złożenia oferty częściowej Wykonawca zobowiązany jest wnieść wadium w kwocie określonej dla danej części. W przypadku złożenia oferty na kilka części kwota wadium stanowi sumę wadiów ustalonych dla poszczególnych części zamówienia. Jeżeli wysokość wniesionego wadium będzie niższa niż suma wynikająca z poszczególnych części zamówienia, Zamawiający uzna, że wadium nie zostało wniesione w wymaganej wysokości.

§ 13
TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą przez 30 dni.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy w sprawie zamówienia publicznego, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawcy o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.
4. Przedłużenie terminu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą. Jeżeli przedłużenie terminu związania ofertą dokonywane jest po wyborze oferty najkorzystniejszej, obowiązek wniesienia nowego wadium lub jego przedłużenia dotyczy jedynie Wykonawcy, którego oferta została wybrana jako najkorzystniejsza.

§ 14
OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Oferta winna zawierać:
   1) wypełniony i podpisany Formularz ofertowy (załącznik nr 1 do SIWZ),
   2) oświadczenia, o których mowa w §10 ust. 1,
   3) dokument potwierdzający umocowanie osoby/osób podpisujących ofertę,

   oraz
   4) w przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia – pełnomocnictwo (w oryginale), które musi zawierać w szczególności wskazanie: oznaczenia postępowania o zamówienie publiczne, którego dotyczy; Wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego; ustanowionego pełnomocnika oraz zakres jego umocowania. *W przypadku złożenia kopii pełnomocnictwa dokument musi być poświadczony notarialnie.* Korespondencja dotycząca postępowania przekazywana będzie do Pełnomocnika,
   5) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik – oryginał pełnomocnictwa – *w przypadku złożenia kopii pełnomocnictwa dokument musi być poświadczony notarialnie* – określający jego zakres. Pełnomocnik posługujący się pełnomocnictwem ma obowiązek złożyć wraz pełnomocnictwem dokument, z którego wynika uprawnienie osób, które udzieliły pełnomocnictwa, do reprezentowania Wykonawcy udzielającego pełnomocnictwa. Korespondencja dotycząca postępowania przekazywana będzie do Pełnomocnika.
2. Wykonawca winien dokładnie zapoznać się ze wszystkimi zapisami SIWZ. Zaleca się, aby Wykonawca zdobył wszelkie informacje, które mogą być konieczne do przygotowania oferty oraz podpisania umowy.
3. Treść oferty musi odpowiadać treści SIWZ i być zgodna z powszechnie obowiązującymi przepisami prawa.
4. Wykonawca może złożyć tylko jedną ofertę pod rygorem odrzucenia.
5. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim, w formie pisemnej na papierze przy użyciu nośnika pisma nie ulegającego usunięciu bez pozostawienia śladów, czytelną techniką. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
6. Zaleca się, aby każda strona oferty była ponumerowana kolejnymi numerami i parafowana, a w Formularzu ofertowym winna być umieszczona informacja z ilu kolejno ponumerowanych stron składa się oferta wraz z załącznikami. Wykonawca może nie podpisywać czystych stron.
7. Strony oferty winny być trwale ze sobą połączone (np. zbindowane, zszyte), z zastrzeżeniem sytuacji opisanej w ust. 11.
8. Wszelkie zmiany w tekście oferty (poprawki, przekreślenia, dopiski) muszą być podpisane przez Wykonawcę pod rygorem ich nieuwzględnienia.
9. Formularz ofertowy oraz załączniki muszą być podpisane przez Wykonawcę lub upełnomocnionego przedstawiciela Wykonawcy.
10. Zamawiający dopuszcza złożenie oferty na formularzach sporządzonych przez Wykonawcę, pod

warunkiem, że ich treść, a także opis kolumn i wierszy odpowiadać będą formularzom określonym przez Zamawiającego.

11. Informacje składane w trakcie postępowania, stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, co do których Wykonawca zastrzega, że nie mogą być udostępniane innym uczestnikom postępowania, muszą być oznaczone klauzulą: *„Dokument stanowi tajemnicę przedsiębiorstwa"*. Informacje te winny być umieszczone w innej osobnej wewnętrznej kopercie, odrębnie od pozostałych informacji zawartych w ofercie. Kartki należy ponumerować w taki sposób, aby umożliwić ich dopasowanie do pozostałej części oferty (należy zachować ciągłość numeracji kartek oferty). Zamawiający uzna informacje zastrzeżone przez Wykonawcę za tajemnicę przedsiębiorstwa zgodnie z kryteriami określonymi w art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.), o ile Wykonawca nie później niż w terminie składania ofert zastrzeże, że nie mogą być one udostępnione oraz wykaże, że są to nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne jego przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których Wykonawca podjął niezbędne działania w celu zachowania ich poufności. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 uPzp.
12. Oferta musi być umieszczona w trwale zamkniętym, nieprzezroczystym i nienaruszonym opakowaniu oznaczonym napisem:

Oferta przetargowa: **„Dzierżawa systemu wirtualizacji serwerów** **Nr postępowania: ZP/1/IV/2017** **Nie otwierać przed terminem: 14.06.2018 r. godz. 13^{00}**

oraz nazwą i dokładnym adresem wraz z numerami telefonów Wykonawcy (dopuszcza się odcisk pieczęci). Wszelkie elementy oferty nie opakowane i nieoznaczone w ten sposób nie będą brane pod uwagę podczas porównania i oceny ofert, a brak informacji dotyczący nazwy przedmiotowego postępowania może być przyczyną otwarcia oferty przed terminem określonym w § 15 ust. 4.

13. Wykonawca może, przed upływem terminu składania ofert, zmienić złożoną przez siebie ofertę. Powiadomienie o zmianie musi być złożone z dopiskiem „Zmiana oferty" według zasad przewidzianych w ust. 12. Po stwierdzeniu poprawności procedury dokonania zmian, zmiany zostaną dołączone do oferty.
14. Wykonawca może, przed upływem terminu składania ofert, wycofać złożoną przez siebie ofertę. Ofertę wycofać może/gą jedynie osoba/y należycie umocowane. W trakcie otwarcia ofert nie będą otwierane oferty, których dotyczy wycofanie, takie oferty zostaną odesłane Wykonawcom na ich wniosek. Wykonawca nie może wycofać oferty i wprowadzić jakichkolwiek zmian w treści oferty po upływie terminu składania ofert.
15. Wykonawca poniesie wszystkie koszty związane z przygotowaniem i złożeniem oferty.

§ 15
MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Oferty należy składać w siedzibie Zamawiającego:
   Lotnicze Pogotowie Ratunkowe, 01-934 Warszawa, ul. Księżycowa 5, sekretariat pokój nr 100 (I piętro)
2. Termin składania ofert upływa **14.06.2018 roku** o **godz. 12^{30}**.
3. Zamawiający dokona otwarcia ofert w siedzibie Zamawiającego:
   Lotnicze Pogotowie Ratunkowe w Warszawie, ul. Księżycowa 5, pokój 111
4. Otwarcie ofert odbędzie się, w obecności Wykonawców, którzy zechcą przybyć do siedziby Zamawiającego w dniu **14.06.2018 roku** o **godz. 13^{00}**.
5. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
6. Podczas otwarcia ofert Zamawiający poda nazwy (firmy) oraz adresy Wykonawców, a także informacje dotyczące ceny i terminu wykonania zamówienia, okresu gwarancji i warunków

płatności zawartych w ofertach.

7. Niezwłocznie po otwarciu ofert Zamawiający zamieści na swojej internetowej www.lpr.com.pl informacje dotyczące:
   a) kwoty, jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,
   b) firm oraz adresów Wykonawców, którzy złożyli ofertę w terminie,
   c) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

§ 16
OPIS SPOSOBU OBLICZENIA CENY

1. Cenę oferty należy określić w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku.
2. Ilekroć mowa o cenie należy przez to rozumieć cenę w rozumieniu art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług.
3. Cena podana przez Wykonawcę w Formularzu ofertowym (załącznik nr 1 do SIWZ) musi być całkowitą ceną brutto za wykonanie zamówienia.
4. Podana przez Wykonawcę cena oferty (wynagrodzenie) będzie wynagrodzeniem ryczałtowym w rozumieniu przepisów ustawy Kodeks cywilny (tekst jednolity Dz. U. z 2017 r. poz. 459 z późn. zm.).
5. Wykonawca określając wynagrodzenie ryczałtowe oświadcza, że wykorzystał wszelkie konieczne środki mające na celu ustalenie wynagrodzenia obejmującego całość prac niezbędnych do wykonania przedmiotu zamówienia.
6. Cena powinna zawierać w sobie ewentualne upusty proponowane przez Wykonawcę.
7. Cena podana przez Wykonawcę nie będzie podlegać żadnym negocjacjom.
8. Cena podana przez Wykonawcę musi zawierać wszelkie koszty związane z realizacją zamówienia i obowiązywać będzie przez cały okres związania ofertą.
9. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

§ 17
INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Rozliczenia prowadzone między Zamawiającym, a Wykonawcą będą prowadzone w PLN.

§ 18
OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY

1. Kryteriami oceny ofert ze wskazaniem procentowego znaczenia tych kryteriów są:

Lp.	Kryterium	Ranga
1.	Cena brutto oferty	**55**
2.	Parametry techniczne	**45**
	Razem	**100**

2. Oferty zostaną ocenione za pomocą systemu punktowego, zgodnie z poniższymi kryteriami:
   1) W kryterium nr 1 – **Cena brutto oferty**, maksymalną liczbę punktów otrzyma oferta z najniższą ceną brutto oferty, natomiast pozostałe oferty otrzymają punkty wynikające z arytmetycznych przeliczeń, zgodnie z poniższym wzorem:

$$C = \frac{C\ \min}{Cob} \times R$$

gdzie: C – liczba punktów przyznanych Wykonawcy w kryterium Cena brutto oferty
Cmin – najniższa zaoferowana Cena brutto oferty
Cob – Cena brutto oferty zaoferowana w badanej ofercie
R – ranga

2) W kryterium nr 2 – **„Parametry techniczne"** maksymalną liczbę punktów, tj. **45** otrzyma Wykonawca, który zaoferuje Zamawiającemu dodatkowy parametr określony w tabeli poniżej. Za każdy dodatkowy parametr Wykonawca uzyska odpowiednią ilość punktów na podstawie oświadczenia Wykonawcy zawartego w Formularzu oferty, w sposób:
   - € **oferuje – 20 pkt albo 10 pkt albo 5 pkt**
   - € **nie oferuje – 0 pkt**

Lp.	Kryterium	Ilość punktów
1.	Pamięć cache pamięci masowej – 16 GB na każdym kontrolerze	20
2.	Dodatkowa pamięć RAM – 32 GB	10
3.	Zainstalowane dyski – dodatkowe 5 dysków każdy o pojemności 6TB	10
4.	Dodatkowe kolejne rdzenie procesora serwera – Tabela 1 – Serwery (Załącznik nr 2 do SIWZ – Opis Przedmiotu Zamówienia)	5
	Razem	**45**

3. W trakcie dokonywania obliczeń Zamawiający zaokrągli każdy z wyników do dwóch miejsc po przecinku.
4. Maksymalna ilość punktów, którą może uzyskać najkorzystniejsza oferta w wyniku oceny według w/w kryteriów wynosi 100 pkt.
5. Za najkorzystniejszą zostanie uznana oferta, która otrzyma najwyższą liczbę punktów.

§ 19
INFORMACJE DOTYCZĄCE AUKCJI ELEKTRONICZNEJ

Zamawiający nie przewiduje w niniejszym postępowaniu wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

§ 20
INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Po wyborze najkorzystniejszej oferty, a przed zawarciem umowy, Zamawiający wezwie Wykonawcę, którego oferta została wybrana do dopełnienia następujących formalności:
   1) osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie wynika z dokumentów załączonych do oferty,
   2) jeżeli wybrana zostanie oferta Wykonawców występujących wspólnie, będą oni zobowiązani, przed zawarciem umowy w sprawie udzielenia zamówienia, do przedstawienia umowy regulującej współpracę tych Wykonawców.
2. Niezłożenie dokumentów, o których mowa w ust. 1 pkt 1) – 2), przez Wykonawcę, którego oferta została wybrana, w wyznaczonym przez Zamawiającego terminie przed podpisaniem umowy, Zamawiający potraktuje jako uchylanie się od zawarcia umowy w sprawie zamówienia publicznego. W takim przypadku, zgodnie z art. 94 ust. 3 uPzp, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzania ich ponownego badania i oceny (chyba że zachodzą przesłanki unieważnienia postępowania, o których mowa w art. 93 ust. 1 uPzp).

§ 21

WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy w przedmiotowym postępowaniu.

§ 22

ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANA WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Istotne postanowienia umowy – załącznik nr 3 do SIWZ.
2. Zgodnie z art. 144 ust. 1 pkt 1) uPzp Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Zmiany, o których mowa w zdaniu poprzednim, zostały przewidziane w załączniku nr 3 do SIWZ – Istotne postanowienia umowy.

§ 23

POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

1. Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów uPzp, przysługują środki ochrony prawnej przewidziane w Dziale VI uPzp, na zasadach i w terminach określonych dla wartości zamówienia równej lub przekraczającej kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 uPzp.
2. Środkami ochrony prawnej są:
   1) odwołanie,
   2) skarga do sądu.
3. Kwestie dotyczące odwołania uregulowane są w art. 180-198 uPzp.
4. Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Kwestie dotyczące skargi do sądu regulowane są w art. 198a-198g uPzp.

§ 24

INFORMACJE DOTYCZĄCE RODO

1. Zamawiający informuje, że na swojej stronie internetowej pod adresem: https://www.lpr.com.pl/pl/rodo/ zamieścił Klauzulę Informacyjną o Przetwarzaniu Danych Osobowych.
2. Obowiązkiem Wykonawcy jest zapoznanie się z treścią Klauzuli oraz złożenie odpowiedniego oświadczenia zawartego w Formularzu oferty – załącznik nr 1 do SIWZ.

§ 25

ZAŁĄCZNIKI DO SIWZ

1. Formularz oferty – załącznik nr 1.
2. Opis przedmiotu zamówienia – załącznik nr 2;
3. Istotne postanowienia umowy – załącznik nr 3;
4. Oświadczenie Wykonawcy składane na podstawie art. 25a ust. 1 uPzp dotyczące przesłanek wykluczenia z postępowania – załącznik nr 4;
5. Oświadczenie Wykonawcy składane na podstawie art. 25a ust. 1 uPzp dotyczące spełniania warunków udziału w postępowaniu – załącznik nr 5;
6. Informacja o przynależności wykonawcy do grupy kapitałowej – załącznik nr 6;

RADCA PRAWNY
Szymon Barusiński
[illegible]

ZAŁĄCZNIK NR 1 DO SIWZ
FORMULARZ OFERTOWY

....., dnia .....

I. INFORMACJE O WYKONAWCY

1. Niniejsza oferta zostaje złożona przez:

.....
nazwa Wykonawcy
.....
.....
adres Wykonawcy (siedziba)

NIP ..... REGON .....

Nr Krajowego Rejestru Sądowego (jeżeli dotyczy) .....

tel. ..... fax .....

e-mail ..... www ..... (jeżeli posiada)

województwo ..... powiat .....

w przypadku oferty wspólnej (Konsorcjum)[1]:

Pełnomocnik Konsorcjum: .....
nazwa Wykonawcy
.....
.....
adres Wykonawcy (siedziba)

NIP ..... REGON .....

Nr Krajowego Rejestru Sądowego (jeżeli dotyczy) .....

tel. ..... fax .....

e-mail ..... www ..... (jeżeli posiada)

województwo ..... powiat .....

Uczestnik Konsorcjum:.....
nazwa Wykonawcy
.....
.....
adres Wykonawcy (siedziba)

NIP ..... REGON .....

Nr Krajowego Rejestru Sądowego (jeżeli dotyczy) .....

[1] *Należy podać nazwy i adresy wszystkich Wykonawców wskazując również Pełnomocnika*

tel. ..... fax .....

e-mail ..... www ..... (jeżeli posiada)

województwo ..... powiat .....

2. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na adres:

.....

nazwa

.....

numer telefonu: .....

numer faksu: .....

adres poczty elektronicznej: .....

II. PRZEDMIOT OFERTY

Nawiązując do ogłoszenia o zamówieniu na „Dzierżawa systemu wirtualizacji serwerów" – nr postępowania ZP/1/IV/2018, my niżej podpisani składamy ofertę w postępowaniu o zamówienie publiczne i:

1. Oferujemy wykonanie przedmiotu zamówienia w zakresie objętym w Specyfikacji Istotnych Warunków Zamówienia (SIWZ) za:

cenę całkowitą brutto ..... PLN, obliczoną zgodnie z poniższym Formularzem cenowym.
cenę całkowitą netto ..... PLN, obliczoną zgodnie z poniższym Formularzem cenowym.

L.p.	Dzierżawa	J.m.	Ilość	Cena jednostkowa netto w PLN	Wartość netto w PLN	Wartość brutto w PLN	Wg stawki podatku VAT w %
A	B	C	D	E	F=DxE	G=FxH	H
1.	Opłata wstępna – 25 % ceny przedmiotu dzierżawy	szt.	1				
2.	Rata dzierżawna równa	mc.	34				
3.	Rata dzierżawna wyrównawcza*	mc.	1				
SUMA całkowity koszt dzierżawy (Zawiera wszystkie opłaty: wpłatę wstępną, wszystkie miesięczne opłaty dzierżawne w ciągu całego okresu trwania dzierżawy, koszty ubezpieczenia)							

** Zamawiający wyraża zgodę na kalkulację ceny z uwzględnieniem ostatniej raty wyrównawczej w przypadku kwoty niepodzielnej na 35 równych rat.* ***Wysokość raty wyrównawczej nie może być większa niż wysokość raty równej, o której mowa w pkt 2 tabeli.*** *W przypadku kwoty podzielnej na 35 równych rat, w pozycji nr 3 tabeli należy wpisać wysokość raty równej w wysokości raty z pkt 2 tabeli.*

Zawarty w cenie całkowitej brutto koszt przedmiotu dzierżawy wynosi:

L.p.	Przedmiot dzierżawy	Cena netto w PLN	Cena brutto w PLN	Wg stawki podatku VAT w %
1.	Przedmiot dzierżawy: System wirtualizacji serwerów Data produkcji ..... Zgodnie z Opisem przedmiotu zamówienia (załącznik nr ..... do SIWZ) oraz Opisem parametrów oferowanego systemu wirtualizacji serwerów (załącznik nr ..... do SIWZ).			

2. Oświadczamy, że w ramach wykonywania przedmiotu zamówienia oferujemy następujące parametry techniczne określone w załączniku nr 2 do SIWZ – Opis Przedmiotu Zamówienia (*należy zaznaczyć znakiem X właściwe oświadczenie*):

L.p.	Opis parametru	Oferuję	Nie oferuję
1.	Pamięć cache pamięci masowej – 16 GB na każdym kontrolerze		
2.	Dodatkowa pamięć RAM – 32 GB		
3.	Zainstalowane dyski – dodatkowe 5 dysków każdy o pojemności 6TB		
4.	Dodatkowe kolejne rdzenie procesora serwera – Tabela 1 – Serwery (Załącznik nr 2 do SIWZ – Opis Przedmiotu Zamówienia)		

W przypadku niezaznaczenia żadnego wiersza, Zamawiający uzna, że Wykonawca nie oferuje dodatkowych parametrów technicznych i przyzna 0 pkt za każdy parametr.

3. Oświadczamy, że udzielamy gwarancji na przedmiot zamówienia na okres ..... miesięcy (*nie mniej niż 36 miesięcy. W przypadku nie uzupełnienia ilości miesięcy przez Wykonawcę, Zamawiający przyjmie 36 miesięczny okres gwarancji*) licząc od chwili produkcyjnego uruchomienia środowiska, potwierdzonego protokołem zdawczo - odbiorczym.
4. Oświadczamy, że[2]:
   - € wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego
   - € wybór naszej oferty prowadził będzie do powstania u Zamawiającego obowiązku podatkowego:

.....

nazwa (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego, wartość bez kwoty podatku.

[2] *Odpowiednie zaznaczyć*

5. Ponadto oświadczamy, że jesteśmy[3]:
   - € mikro przedsiębiorcą, tj. zatrudniamy <10 osób, a roczny obrót lub roczna suma bilansowa wynosi < 2 mln euro,
   - € małym przedsiębiorcą, tj. zatrudniamy <50 osób, a roczny obrót lub roczna suma bilansowa wynosi < 10 mln euro,
   - € średnim przedsiębiorcą, tj. zatrudniamy <250 osób, a roczny obrót wynosi < 50 mln euro lub roczna suma bilansowa wynosi < 43 mln euro.
6. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (wraz z załącznikami stanowiącymi jej integralną cześć) oraz wyjaśnieniami i zmianami SIWZ przekazanymi przez Zamawiającego i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
7. Oświadczamy, że zapoznaliśmy się z Istotnymi postanowieniami umowy, które stanowią załącznik nr 3 do SIWZ i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na określonych w tym załączniku warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.
8. Osoby uprawnione do kontaktowania się w sprawach wykonania przedmiotu umowy ze strony Wykonawcy: p. ....., tel. ....., e-mail ..... .
9. Zamówienie wykonamy sami/ wykonanie następujących części zamówienia powierzymy podwykonawcom[4].
10. Oświadczamy, że powierzymy podwykonawcom część zamówienia:

Część zamówienia	Nazwa (firma) podwykonawcy

11. Uważamy się za związanych niniejszą ofertą na czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, czyli przez okres 30 dni od upływu terminu składania ofert.
12. Wadium zostało wniesione:
    - € w pieniądzu na rachunek bankowy Zamawiającego
    - € w siedzibie Zamawiającego w formie .....[5]
13. Prosimy o zwrot wadium (wniesionego w pieniądzu), na zasadach określonych w art. 46 uPzp, na następujący rachunek bankowy .....[6]
14. Oświadczamy, że na podstawie art. 8 ust. 3 uPzp[7]:
    - € żadne z informacji zawartych w ofercie oraz załączonych do niej dokumentach, nie stanowią tajemnicy przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji,
    - € wskazane poniżej informacje zawarte w ofercie oraz załączonych do niej dokumentach, stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i w związku z niniejszym nie mogą być one udostępniane, w szczególności innym uczestnikom postępowania.

Lp.	Oznaczenie rodzaju (nazwy) informacji	Strony w ofercie (wyrażone cyfrą)	
		od	do

[3] *Odpowiednie zaznaczyć*
[4] *Niepotrzebne skreślić*
[5] *Podać formę wniesionego wadium, inną niż pieniądz*
[6] *Jeżeli dotyczy*
[7] *Niepotrzebne skreślić*

Uwaga! W przypadku braku wykazania (złożenia właściwego uzasadnienia w terminie składania ofert), iż zastrzeżone dane stanowią tajemnicę przedsiębiorstwa, Zamawiający uzna, iż nie została spełniona przesłanka podjęcia niezbędnych działań w celu zachowania ich poufności i dane te staną się jawne od momentu otwarcia ofert.

15. Oświadczamy, że spełniamy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[8] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.[9]
    Jednocześnie przyjmujemy do wiadomości, że szczegółowe informacje dotyczące RODO znajdują się na stronie internetowej Zamawiającego pod adresem: https://www.lpr.com.pl/pl/rodo/
16. Oferta została złożona na …….. zapisanych stronach, kolejno ponumerowanych od nr …… do ……..
17. Niniejszym potwierdzam załączenie do oferty następujących dokumentów:
    (numerowany wykaz załączników wraz z tytułami)

    1) ..... *Załącznik nr .....*
    2) ..... *Załącznik nr .....*

.....
Podpis (y) Wykonawcy (ów) lub
upoważnionego(ych) przedstawiciela(li)
Wykonawcy(ów)

[8] *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).*

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

ZAŁĄCZNIK NR 4 DO SIWZ

Zamawiający:
Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5, 01-934 Warszawa

Wykonawca:

.....
(pełna nazwa/firma, adres)

OŚWIADCZENIE WYKONAWCY
SKŁADANE NA PODSTAWIE ART. 25A UST. 1 uPZP
DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dzierżawa systemu wirtualizacji serwerów"** – nr postępowania **ZP/1/IV/2018** prowadzonego przez Lotnicze Pogotowie Ratunkowe, oświadczam, co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

1) Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie § 9 ust. 2 SIWZ (art. 24 ust. 1 pkt 12-23 uPzp).

..... *(miejscowość),* dnia ..... r. .....
(podpis Wykonawcy)

OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:

1. .....
2. .....
... .

(Firma, adres)

nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

..... *(miejscowość),* dnia ..... r. .....

(podpis Wykonawcy)

OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami:

1. .....
2. .....
... .

(Firma, adres)

nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia.

..... *(miejscowość),* dnia ..... r. .....

(podpis Wykonawcy)

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.

..... *(miejscowość),* dnia ..... r. .....

(podpis Wykonawcy)

ZAŁĄCZNIK NR 5 DO SIWZ

Zamawiający:
Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5, 01-934 Warszawa

Wykonawca:

.....
(Firma, adres)

OŚWIADCZENIE WYKONAWCY
SKŁADANE NA PODSTAWIE ART. 25A UST. 1 UPZP
DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Dzierżawa systemu wirtualizacji serwerów"** *(Nr postępowania ZP/1/IV/2018)*, prowadzonego przez Lotnicze Pogotowie Ratunkowe, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w § 9 ust. 1 Specyfikacji Istotnych Warunków Zamówienia, tj.

1. Posiadam doświadczenie w wykonaniu przedmiotu zamówienia / polegam na doświadczeniu podmiotu ..... zgodnie z poniższym wykazem*:

Lp.	Przedmiot zamówienia (opis wykonanej dostawy)	Data wykonania zamówienia		Nazwa i adres odbiorcy-Zleceniodawcy
		początek (data)	zakończenie (data)	
1	2	3		4
1.				
2.				

* *niepotrzebne skreślić*

2. Skieruję do wykonania przedmiotu zamówienia nw. osoby:

Lp.	Imię i nazwisko	Pełniona funkcja	Informacje dotyczące kwalifikacji zawodowych (uprawnienia)	Informacja o podstawie do dysponowania osobami
1.				dysponuję podstawa dysponowania osobą - umowa o pracę* - umowa zlecenie* - inne (podać jakie)* .....:..... będę dysponował* - zobowiązanie innego podmiotu
2.				dysponuję podstawa dysponowania osobą - umowa o pracę* - umowa zlecenie* - inne (podać jakie)* .....:..... będę dysponował* - zobowiązanie innego podmiotu

..... *(miejscowość),* dnia ..... r. .....

(podpis Wykonawcy)

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w § 9 ust. 1 Specyfikacji Istotnych Warunków Zamówienia, polegam na zasobach następującego/ych podmiotu/ów:

L.p.	**Nazwa podmiotu** *(Firma, adres)*	**Zakres polegania zasobach podmiotu**

..... *(miejscowość),* dnia ..... r. .....

(podpis Wykonawcy)

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.

..... *(miejscowość)*, dnia ..... r. .....

(podpis Wykonawcy)

ZAŁĄCZNIK NR 6 DO SIWZ

INFORMACJA O PRZYNALEŻNOŚCI WYKONAWCY DO GRUPY KAPITAŁOWEJ

.....
(pełna nazwa i adres Wykonawcy)

Na podstawie art. 24 ust. 11 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych oświadczam, że: **należę / nie należę**[10] do tej samej grupy kapitałowej co inni Wykonawcy, którzy złożyli odrębne oferty, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2017 r. poz. 229 z późn. zm.), w postępowaniu pn. **„Dzierżawa systemu wirtualizacji serwerów"** – nr postępowania **ZP/1/IV/2018.**

....., dnia ....

Podpis (y) Wykonawcy (ów) lub
upoważnionego(ych) przedstawiciela(li)
Wykonawcy(ów)

W przypadku, gdy Wykonawca **należy** do tej samej grupy kapitałowej co inni Wykonawcy którzy złożyli odrębne oferty w przedmiotowym postępowaniu wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

Uwaga:
W przypadku złożenia oferty przez podmioty występujące wspólnie, wymagane oświadczenie winno być złożone przez każdy podmiot.

[10] *niepotrzebne skreślić*

ZAŁĄCZNIK NR 2 DO SIWZ – OPIS PRZEDMIOTU ZAMÓWIENIA (po zmianach z dnia 6.06.2018 r.)

Wydzierżawiający w ramach realizacji umowy zobowiązany jest do:

1. Udostępnienia fizycznych serwerów o parametrach nie gorszych niż wskazane w Tabeli 1 w ilości 2 sztuk na okres 3 lat.
2. Udostępnienia pamięci masowej o parametrach nie gorszych niż wskazane w Tabeli 2 w ilości 1 sztuki na okres 3 lat.
3. Udostępnienia przełączników sieciowych o parametrach nie gorszych niż wskazane w Tabeli 3 w ilości 2 sztuk na okres 3 lat.
4. Zapewnienia Dzierżawcy, licencji oprogramowania dla wirtualizacji fizycznych serwerów w ilości odpowiadającej łącznej ilości procesorów fizycznych serwerów określonych w Tabeli 1 wraz z 3 letnim uprawnieniem do uzyskania aktualizacji, nowych wersji oprogramowania oraz wsparcia technicznego producenta oprogramowania lub podmiotu przez niego uprawnionego. Wymagania dotyczące minimalnych wymaganych funkcjonalności określono w tabeli 4.
5. Zapewnienia Dzierżawcy, licencji oprogramowania dla zarządzania oprogramowaniem dla wirtualizacji fizycznych serwerów w wersji odpowiadającej możliwość zarządzania środowiskiem dla co najmniej czterech serwerów fizycznych określonych w Tabeli 1 wraz z 3 letnim uprawnieniem do uzyskania aktualizacji, nowych wersji oprogramowania oraz wsparcia technicznego producenta oprogramowania lub podmiotu przez niego uprawnionego.
6. Instalacji, konfiguracji oraz aktualizacji oprogramowania udostępnianej infrastruktury oraz wykonania usług związanych z migracją istniejących serwerów wirtualnych w ilości minimum 37 szt. wraz z migracją danych zapisanych na aktualnie eksploatowanej pamięci masowej. Dzierżawca informuje, że aktualnie eksploatuje środowisko oparte na oprogramowaniu VMWare 5.5 Enterprise Plus, oparte na dwóch fizycznych serwerach, przełącznikach sieciowych w technologii Fiber Channel oraz pamięć masową posiadającą pojemność użytkową 12 TB. Wydzierżawiający zobowiązany jest przeprowadzić migrację posiadanych przez Dzierżawcę zasobów do nowego środowiska w sposób minimalizujący czas niedostępności i przestojów. Wydzierżawiający winien w terminie 14 dni od podpisania Umowy przedstawić Dzierżawcy planowany scenariusz migracji, a Dzierżawca w terminie kolejnych 7 zatwierdzić lub wnieść uwagi.

Wymagania ogólne dla udostępnianego sprzętu i oprogramowania:

1. Wszystkie urządzenia udostępniane Dzierżawcy muszą być fabrycznie nowe i wyprodukowane nie później niż 6 miesięcy przed datą dostawy.
2. Wszystkie urządzenia udostępniane Dzierżawcy muszą być objęte min. 36 miesięczną gwarancją producenta, a Dzierżawca musi zachować prawo do bezpośredniego kontaktu z producentem sprzętu udostępnionego przez Wydzierżawiającego.
3. Serwis gwarancyjny dla urządzeń udostępnianych przez Wydzierżawiającego musi zapewniać prawo do składania zleceń związanych z serwisem 24 godziny na dobę przez 7 dni w tygodniu. Obsługa serwisowa musi być realizowana za pośrednictwem dedykowanego oprogramowania dla obsługi sprzętu udostępnionego. Gwarantowany czas usunięcia awarii przez producenta lub jego upoważnionego przedstawiciela nie może przekroczyć 24 godzin. W całym okresie trwania gwarancji wszystkie usługi serwisu gwarancyjnego mają być świadczone w siedzibie Dzierżawcy. Dzierżawca nie

dopuszcza dostawy sprzętu zastępczego na czas wykonania naprawy o parametrach innych niż ujęte w zgłoszeniu tj. Dzierżawca, z uwagi na specyfikę środowiska, nie dopuszcza podstawienia sprzętu o innych parametrach.

4. Wydzierżawiający zobowiązany jest dostarczyć wszystkie elementy komunikacyjne pochodzące od producenta oferowanego sprzętu.
5. Udostępniany sprzęt wskazany z tabeli 1, 2 oraz 3 winien pochodzić od tego samego producenta. W przypadku zaoferowania sprzętu pochodzącego od różnych producentów Wydzierżawiający zobowiązany jest załączyć do oferty oświadczenia producentów w zakresie kompatybilności oferowanego sprzętu.
6. Wydzierżawiający zobowiązany jest do wskazania konkretnych parametrów sprzętu i oprogramowania będącego przedmiotem oferty w sposób umożliwiających ich identyfikację w sposób jednoznaczny i niebudzący wątpliwości.

Tabela 1 - Serwery

Nazwa elementu, parametru lub cechy	Opis wymagań	Parametry dodatkowo punktowane
Ilość sztuk	2 szt.	
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 2U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych	Nie dotyczy
Procesor	Architektura x86, maksymalny TDP dla procesora 85W. Co najmniej 8 rdzeni w każdym procesorze. Wynik wydajności procesora instalowanego w oferowanym serwerze, w konfiguracji dwuprocesorowej, powinien wynosić co najmniej 60,4 punktów w SPEC w teście SPECint2006 Results -- Results opublikowanych przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów.	Dodatkowe, kolejne, rdzenie – 1 punkt za każde 2. Maksymalnie 5 punktów
Liczba zainstalowanych procesorów	Min. 2	Nie dotyczy
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością	Nie dotyczy

	zainstalowania co najmniej dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)	
Pamięć operacyjna	Zainstalowane co najmniej 128 GB pamięci RAM co najmniej DDR4 w modułach o pojemności co najmniej 16GB każdy, o taktowaniu co najmniej 2666MHz. Minimum 24 sloty na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Pamięć o częstotliwości co najmniej 2666MHz. Możliwość rozbudowy RAM do co najmniej 3TB (dopuszcza się wymianę modułów pamięci)	Każde dodatkowe 32 GB zainstalowanej pamięci RAM – 5 pkt. Maksymalnie 10 pkt.
Zabezpieczenie pamięci	ECC, Memory Mirroring, Memory Rank Sparing, Patrol Scrubbing oraz Demand Scrubbing.	Nie dotyczy
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz z głębią koloru co najmniej 16 bitów/piksel.	Nie dotyczy
Dyski	Zainstalowane dyski na system operacyjny: - 2 dyski M.2, skonfigurowane w RAID 1, o pojemności co najmniej 32GB każdy. Wymagana jest możliwość zastosowania w obudowie serwera modułu dyskowego (lub modułów dyskowych), którego gniazda dyskowe pozwalają na zamienne zastosowanie dysków SAS/SATA 2,5" oraz dysków NVMe w formacie 2,5" w tym samym gnieździe dyskowym, z możliwością uzyskania co najmniej 8 takich gniazd dyskowych w pojedynczym serwerze.	Nie dotyczy

Zasilacz	Minimum dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie przekraczającej 750W, z certyfikatem minimum Platinum.	Nie dotyczy
Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne interfejsy: - co najmniej 1 port 10/100/1000 Ethernet RJ-45 dedykowany do celów administracyjnych - co najmniej 2 porty 10Gbps Ethernet SFP+ SR, rozłożone równo pomiędzy co najmniej dwie niezależne od siebie karty. Wszystkie karty LAN 10Gbps muszą być zbudowane z zastosowaniem technologii tego samego producenta. - co najmniej 2 porty 16Gbps FC, rozłożone równo pomiędzy co najmniej dwie niezależne od siebie karty. Wszystkie karty FC muszą być zbudowane z zastosowaniem technologii tego samego producenta.	Nie dotyczy
Dodatkowe porty	• z przodu obudowy: 1x USB 3.0, 1x USB 2.0 z dostępem dla podsystemu zarządzania (modułu administracyjnego) serwera, niezależnie od zainstalowanego systemu operacyjnego. • z tyłu obudowy: 2x USB 3.0, 1x DB-15 VGA.	Nie dotyczy
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1	Nie dotyczy

Zarządzanie	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania, umożliwiający: • Zbieranie i przeglądanie informacji o systemie oraz inwentaryzacja • Monitorowanie statusu systemu oraz jego stanu • Podnoszenie alarmów oraz wysyłanie informacji • Zapisywanie zdarzeń w dzienniku • Konfigurowanie połączeń sieciowych • Konfigurowanie bezpieczeństwa • Aktualizowanie oprogramowania wewnętrznego (firmware) • Konfigurowanie ustawień serwera oraz urządzeń • Monitorowanie zużycia energii elektrycznej w czasie rzeczywistym • Zdalne kontrolowanie zasilania serwera (włączenie, wyłączenie, restart) • Zarządzanie kluczami aktywacyjnymi funkcji na żądanie (FoD) • Przekierowywanie konsoli szeregowej poprzez IPMI • Przechwytywanie treści wyświetlanej na konsoli w przypadku zawieszenia się systemu operacyjnego	Nie dotyczy

	• Zdalny podgląd treści konsoli w rozdzielczości co najmniej 1920x1200 przy odświeżaniu z częstotliwością 60 Hz i głębią koloru co najmniej 16 bitów / piksel • Zdalny dostęp do serwera z użyciem klawiatury i myszy zdalnej stacji klienckiej • Zdalne instalowanie systemu operacyjnego • Alarmowanie za pośrednictwem Syslog • Przekierowanie konsoli szeregowej poprzez SSH • Wyświetlanie grafiki z danymi w czasie rzeczywistym oraz z danymi historycznymi na temat poboru mocy i temperatury • Ograniczanie poboru mocy • Mapowanie obrazu ISO i plików obrazów nośników, zlokalizowanych w lokalnej stacji klienckiej jako wirtualnych napędów, dostępnych do użycia przez serwer • Montowanie zdalnych obrazów ISO I plików obrazów nośników poprzez HTTPS, SFTP, CIFS i NFS • Współpraca co najmniej sześciu użytkowników konsoli wirtualnej • Kontrolowanie jakości i wykorzystania pasma komunikacyjnego • Obsługa co najmniej następujących interfejsów komunikacyjnych: IPMI v2.0, SNMP v3, CIM, DCMI v 1.5, REST API, WWW na bazie HTML 5, CLI (wiersz komend).	

	• Dostęp przy pomocy smartfona z systemem Android oraz z systemem iOS, z zainstalowaną aplikacją, dostarczaną przez producenta serwera, poprzez port USB z przodu serwera, z możliwością co najmniej sprawdzenia stanu i statusu serwera, poziomu firmware, ustawień sieciowych i alarmów, a także z możliwością włączenia, wyłączenia i zrestartowania serwera. Ze względów bezpieczeństwa, nie dopuszcza się komunikacji bezprzewodowej pomiędzy serwerem a smartfonem.	
Funkcje zabezpieczeń	Hasło włączania, hasło administratora, moduł TPM z możliwością przełączania w UEFI pomiędzy wersją 1.2 a 2.0. Możliwość zastosowania zamykanego na klucz panelu przedniego serwera.	Nie dotyczy
Urządzenia hot swap	Co najmniej dyski, zasilacze oraz wentylatory	Nie dotyczy
Obsługa	Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych.	Nie dotyczy
Diagnostyka	Wbudowany system analizy predykcyjnej, pozwalający na przewidywanie możliwości wystąpienia awarii serwera. Analiza musi obejmować co najmniej: procesory, regulatory napięcia, pamięć operacyjną (RAM), dyski wewnętrzne, wentylatory, zasilacze, kontrolery RAID Możliwość użycia aplikacji mobilnej na smartfonie z systemem Android oraz iOS, podłączonym do serwera poprzez port USB z przodu obudowy, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. Odpowiednie licencje należy uwzględnić w ofercie.	Nie dotyczy

Wspierane systemy operacyjne	Microsoft Windows Server 2012 R2 i 2016, Red Hat Enterprise Linux 6 oraz 7, SUSE Linux Enterprise Server 11 oraz 12, VMware vSphere (ESXi) 6.0 oraz 6.5.	Nie dotyczy
Waga	Nie więcej niż 32 kg w maksymalnej możliwej konfiguracji serwera.	Nie dotyczy
Gwarancja i serwis	Co najmniej 36 miesięcy gwarancji producenta. Obsługa 24 godziny na dobę, 7 dni w tygodniu. Gwarantowany czas naprawy 24h. Wszelkie uszkodzone nośniki danych pozostają u Dzierżawcy. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie „Diagnostyka" (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji do 36 miesięcy 7/24 fix 4h oraz zainstalowania dodatkowego dla każdej lokalizacji systemu monitoringu (na dedykowanym serwerze o parametrach rekomendowanych przez producenta oprogramowania monitorującego). Możliwość generowania zleceń serwisowych w dedykowanej aplikacji bezpośrednio połączonej z systemem obsługi technicznej dostawcy pozwalającej na nadawanie odpowiednich uprawnień operatorom a także zapewniający fizyczny sprzętowy klucz uwierzytelnienia operatora. Niezbędne licencje należy uwzględnić w ofercie.	Nie dotyczy

Tabela 2 – Pamięć masowa

Nazwa elementu, parametru lub cechy	Opis wymagań	Parametry dodatkowo punktowane
Pamięć masowa	Pamięć masowa musi zostać dostarczona w postaci pamięci masowej produkcyjnej.	Nie dotyczy
Obudowa	Do montażu w szafie rack 19", obudowa kontrolera o wysokości nie większej niż 2U, umożliwiająca instalację co najmniej 24 dysków 2,5". Obudowa zawierająca kontrolery musi również zawierać gniazda do instalacji co najmniej 24 dysków 2,5".	Nie dotyczy
Zainstalowane dyski	- Co najmniej 5 dysków HotSwap SSD o pojemności co najmniej 400GB każdy - Co najmniej 19 dysków HotSwap HDD o pojemności co najmniej 900GB każdy, o prędkości obrotowej co najmniej 10k rpm	Zestaw 5 dodatkowych dysków twardych typu NL-SAS 7200 obrotów na minutę o pojemności min 6TB – 10 punktów
Zasilanie	Co najmniej dwa zasilacze 230V/50Hz, pracujące redundantnie, Zasilacze muszą posiadać możliwość wymiany bez zatrzymywania pamięci masowej tzw. Hot Swap.	Nie dotyczy
Kontrolery	Co najmniej dwa kontrolery, pracujące redundantnie. Kontrolery muszą być posiadać możliwość wymiany bez zatrzymywania pamięci masowej tzw. Hot Swap.	Nie dotyczy
Obsługiwane grupy RAID	Co najmniej RAID 0, 1, 5, 6, 10	Nie dotyczy
Pamięć cache	Co najmniej po 8GB na każdym kontrolerze - mirroring pomiędzy kontrolerami. Wymagane zabezpieczenie pamięci cache przed utratą zawartości przy utracie zasilania.	16GB na każdym kontrolerze mirroring pomiędzy kontrolerami. Wymagane zabezpieczenie pamięci cache przed utratą zawartości przy utracie zasilania – dodatkowe 20 pkt
Możliwość rozbudowy systemu dyskowego	Dostępność półek dyskowych na dyski 2,5" oraz na dyski 3,5" z możliwością mieszania półek na dyski 2,5" i dyski 3,5" w tej samej macierzy dyskowej. Możliwość dołączenia co najmniej	Nie dotyczy

	10 dodatkowych półek dyskowych do półki z kontrolerami, przy zachowaniu redundancji połączeń.	
Sposób podłączenia dodatkowych półek dyskowych	Każda dodatkowa półka dyskowa musi posiadać dwa pracujące redundantnie moduły komunikacyjne Hot Swap. Dodatkowa półka dyskowa musi być podłączona do macierzy dyskowej co najmniej dwoma pracującymi redundantnie połączeniami, każde w technologii SAS 12Gbps lub szybszej, przy czym każda półka dyskowa musi komunikować się z każdym kontrolerem.	Nie dotyczy
Rozbudowa pojemności	Rozbudowa pojemności pamięci masowej w zakresie zarówno instalowania dodatkowych dysków jak również dodatkowych półek dyskowych musi odbywać się bez konieczności zakupu dodatkowych licencji z tytułu rozbudowy pojemności/dokładania kolejnych dysków. W przypadku zaoferowania pamięci masowej objętej koniecznością zakupu licencji oprogramowania na rozbudowę pamięci masowej dostawca winien uwzględnić w cenie ich koszt dla deklarowanej przez producenta pojemności.	Nie dotyczy
Sposób podłączenia dysków do kontrolerów	Każdy dysk podłączony dwoma portami SAS 12Gbps, po jednym porcie do każdego kontrolera pamięci masowej. W przypadku dodatkowych półek dyskowych każdy dysk musi być podłączony dwoma portami SAS 12Gbps, po jednym porcie do każdego modułu komunikacyjnego w półce dyskowej. Wszystkie dyski muszą być Hot Swap.	Nie dotyczy
Interfejsy komunikacyjne do podłączenia hostów	- Co najmniej po dwa porty 1Gbps Ethernet z obsługą iSCSI na każdym kontrolerze. - Co najmniej po dwa porty SAS 12Gbps na każdym kontrolerze - Co najmniej po cztery porty 16Gbps FC na każdym kontrolerze. Porty FC musza być w standardzie SFP+ i muszą być obsadzone wkładkami optycznymi 16Gbps SW ze	Nie dotyczy

	złaczami LC. Wkładki muszą zapewniać funkcjonalność wymiany bez zatrzymywania pamięci masowej tzw. Hot Swap.	
Wymagane funkcje kontrolerów - wymienione funkcje muszą być obecne w oferowanej macierzy i gotowe do użycia.	Thin Provisioning, kopie migawkowe (snapshoty) - co najmniej 64 relacje źródło - cel. Jednorazowa migracja danych z zewnętrznej macierzy dyskowej, w tym macierzy innego producenta niż oferowana macierz. Wykonywanie kopii synchronicznej danych z jednej macierzy na drugą pamięć masową tej samej rodziny. Grupy RAID 5 i RAID 6 z dyskami zapasowymi (spare disk). W grupach RAID 5 oraz RAID 6 z dyskami zapasowymi (spare drive) dyski zapasowe muszą być używane podczas normalnej pracy macierzy do zapisu danych, a przestrzeń zapasowa musi być rozdystrybuowana na wszystkie dyski w grupie RAID. Grupa RAID z rozdystrybuowaną przestrzenią zapasową musi umożliwiać obsługę co najmniej 128 dysków w jednej grupie RAID. Funkcja tieringu danych pomiędzy dyskami HDD i SSD. Macierz musi umożliwiać migrację danych z zewnętrznej macierzy dowolnego producenta, wyposażonej w interfejsy FC i udostępniającej dane standardowym protokołem FC. Migracja danych musi się odbywac z zastosowaniem wyłącznie metod dostępnych w oferowanej macierzy, bez pomocy zewnętrznego oprogramowania. Proces migracji danych z zewnętrznej macierzy na zasoby własne oferowanej macierzy musi przebiegać w taki sposób, aby hosty podłączone do oferowanej macierzy, a nie podłączone do zewnętrznej macierzy, mogły korzystać z migrowanych danych w trakcie ich migracji. Oprogramowanie do realizacji zdalnej replikacji na macierz tego samego rodzaju dla całej proponowanej konfiguracji.	Nie dotyczy

	Wymagane jest zapewnienie niezbędnych do tych celów licencji oprogramowania na okres min 3 lat.	
Wymagane możliwości rozbudowy funkcji macierzy - wymienione funkcje muszą być dostępne do zakupienia w chwili oferowania macierzy lub obecne w oferowanej macierzy	Możliwość zwiększenia liczby relacji źródło - cel dla kopii migawkowych do co najmniej 2000.	Nie dotyczy
Wymagana liczba udostępnianych wolumenów logicznych	nie mniej niż 2000	Nie dotyczy
Wymagana wielkość logicznego wolumenu	nie mniej niż 256TB	Nie dotyczy
Wymagana liczba grup RAID	nie mnie niż 128	Nie dotyczy
Wymagana liczba obsługiwanych hostów	nie mniej niż 256	Nie dotyczy

Wymagana liczba portów per host	nie mniej niż 32	Nie dotyczy
Wymagany dostęp administracyjny	Dwa porty 1Gbps Ethernet (po jednym na każdym kontrolerze) - porty mogą być te same co do obsługi iSCSI. Dostęp przez WEB-based GUI oraz SSH CLI oraz SMI-S oraz SNMP oraz notyfikacje poprzez e-mail.	Nie dotyczy
Wymagane metody zabezpieczenia dostępu administracyjnego	SSL oraz SSH oraz autentykacja LDAP.	
Serwis	co najmniej 3 lata, zgłaszanie problemów 24h na dobę, 7 dni w tygodniu, z gwarantowanym czasem naprawy w 24 godziny w miejscu eksploatacji. Wymieniane dyski pozostają u Dzierżawcy.	Nie dotyczy

Tabela 3 – Przełącznik Fibre Channel – 2 sztuki

Nazwa elementu, parametru lub cechy	Opis wymagań	Parametry dodatkowo punktowane
Obudowa	Przeznaczona do montażu w szafie rack 19", o wysokości nie większej niż 1U. Obudowa musi być wyposażona we wszystkie elementy, niezbędne do zamontowania przełącznika w szafie rack 19".	Nie dotyczy
Porty	Co najmniej 24 gniazda na wkładki SFP+. Co najmniej 12 gniazd aktywnych i obsadzonych wkładkami 16Gbps FC, wielomodowymi, o zasięgu co najmniej 125m przy zastosowaniu światłowodu OM4 i przy prędkości transmisji 16Gbps. Aktywacja dodatkowych portów realizowana wyłącznie programowo za pośrednictwem odpowiednich licencji.	Nie dotyczy

	Wkładki SFP+ 16Gbps FC musza obsługiwać autosensing i muszą automatycznie dostosowywać się do pracy z przepustowościami 4Gbps, 8Gbps i 16Gbps.	
Obsługiwane typy portów	Obsługa trybu Full Fabric oraz trybu Access Gateway. Jesli wymagane odpowiednie licencje nalezy uwzględnić. Obsługa portów FL_Port, F_Port, M_Port, E_Port, D_Port oraz N_Port NPIV.	Nie dotyczy
Obsługiwane rodzaje ruchu	Unicast, Multicast, Broadcast	Nie dotyczy
Class of Service	Class 2, Class 3 oraz Class F	Nie dotyczy
Zagregowana przepustowość	Co najmniej 384Gbps	Nie dotyczy
Zużycie energii	Nie więcej niż 3.4 watt na port zdefiniowany jako 16Gbps	Nie dotyczy
Port Zarządzania	Dedykowany do obsługi przełącznika min 10/100Mbps port w standardzie RJ45 oraz modulowany RS232 w oparciu o niezależny port fizyczny w standardzie RJ45	Nie dotyczy
Port USB	Wymagany, dostępny od strony portów dostępowych przełącznika	Nie dotyczy
Opóźnienia	Nie większe niż 0,7 mikrosekundy (dopuszcza się wzrost do 1,1 mikrosekundy w przypadku włączenia FEC	Nie dotyczy
Zasilanie I chłodzenie	Dwa zasilacze. Każdy z zasilaczy wyposażony w min 2 wentylatory pracujące w trybie 2+2.	Nie dotyczy
Gwarancja	3 lata, 24x7, gwarantowany czas naprawy 24h. Gwarancja obejmuje uprawnienia do aktualizacji oprogramowania.	Nie dotyczy

Tabela 4 – Oprogramowanie do wirtualizacji serwerów fizycznych i zarządzania środowiskiem wirtualnym

Wymagane jest dostarczenie licencji na oprogramowanie VMware vSphere ESXi, w najnowszej dostępnej wersji, dla minimum 4 fizycznych CPU (lub większej w przypadku zaoferowania serwerów z większą ilością zainstalowanych procesorów niż 2 na serwer) z funkcjonalnościami:	
a)	Wirtualizator środowiska instalowany bezpośrednio na warstwie fizycznej umożliwiający współdzielenie zasobów sprzętowych typu procesor, pamięć, dysk, karta sieciowa przez różne systemy operacyjne
b)	Sposób licencjonowania środowiska umożliwiający rozbudowę o kolejne fizyczne serwery bez potrzeby uprzedniej aktualizacji już działającego oprogramowania.
c)	Technologia zapewniania wysokiej dostępności przy wykorzystaniu mechanizmu High Availability oraz Fault Tolerance. Technologia Fault Tolerance realizowana od 2 do 4 wirtualnych procesorów.
d)	Technologia automatycznego przenoszenia działających maszyn wirtualnych w obrębie dostępnej infrastruktury wirtualnej dla równoważenia obciążenia poszczególnych maszyn wirtualnych
e)	Technologia umożliwiająca uruchamianie wirtualnych przełączników sieci LAN
f)	Technologia umożliwiająca przenoszenie działających maszyn wirtualnych pomiędzy fizycznymi serwerami działającymi w ramach środowiska wirtualnego bez utraty działających usług i bez konieczności planowania przerw w działaniu maszyny wirtualnej
g)	Technologia zapewniająca szyfrowanie maszyn wirtualnych zarówno w obszarze przydzielonej puli dyskowej jak również danych aplikacji.
h)	Technologia optymalizująca zużycie energii poprzez automatyczne przenoszenie działających maszyn wirtualnych pomiędzy serwerami oraz wyłączanie niewykorzystywanych serwerów.
i)	Technologia nadawania priorytetów dostępu do puli dyskowych maszyn wirtualnych poprzez monitoring obciążenia I/O dla woluminów dyskowych z jednoczesną, dynamiczną, priorytetyzacją ruchu dla wybranych maszyn wirtualnych.
j)	Technologia obniżająca opóźnienia w ruchu sieciowym poprzez prezentowanie pojedynczego fizycznego adaptera serwera fizycznego jako wielu odseparowanych logicznych adapterów dla maszyn wirtualnych.

k)	Technologia proaktywnego przenoszenia działających maszyn wirtualnych pomiędzy fizycznymi serwerami pracującymi w środowisku na wypadek detekcji /wykrycia potencjalnej awarii zasobu sprzętowego.
l)	technologia pozwalająca na jednoczesne połączenie z zasobami sieci SAN za pomocą wielu światłowodów (multipathing),
m)	technologia pozwalająca na wirtualizację aplikacji,
n)	Technologia umożliwiająca przechowywanie konfiguracji i ustawień dla poszczególnych wirtualnych maszyn umożlwiająca ich przechowywanie jako wzorzec dla innych hostów środowiska.
o)	Technologia monitorowania zmian konfiguracji poszczególnych hostów zapewniająca automatyczne powiadomienia dla administratora
p)	Technologia udostępniania natywnej wydajności kart graficznych opatrzonych koprocesorami 2D/3D dla maszyn wirtualnych (vGPU)
q)	technologia pozwalająca na tworzenie wirtualnych, rozproszonych przełączników sieciowych,
r)	oprogramowanie serwera (licencja na 1 CPU, dla MS Windows Server 2012 lub nowszy) zapewniające ujednolicone zarządzanie za pomocą jednej konsoli wszystkimi hostami oraz urządzeniami wirtualnymi w środowisku wirtualnym Dzierżawcy, umożliwiające administratorom kontrolę nad środowiskiem i ułatwiające wykonywanie codziennych zadań, zgodne z wersją dostarczonego środowiska,
s)	Wraz z oprogramowanie realizującym powyższe funkcjonalności Wydzierżawiający zapewni oprogramowanie zarządzające dedykowane dla administrowania środowiskiem. Oprogramowanie do zarządzania musi za pośrednictwem dedykowanej konsoli instalowanej na serwerach dostarczonej infrastruktury prezentować wszystkie zdefiniowanie maszyny wirtualne oraz umożliwiać administrowanie zasobami maszyn wirtualnych za pośrednictwem panelu administratora. Konsola zarządzania środowiskiem musi udostępniać usługi co najmniej dla wszystkich serwerów fizycznych dostarczonych dla potrzeby zadania a także zapewnić:
	i. Umożliwić działanie odrębnej instancji wirtualnego serwera zarządzania co najmniej w konfiguracji zapewniającej ciągłość dostępu do konsoli na wypadek awarii (funkcjonalność failover)
	ii. Umożliwić prezentację treści wielu instancji konsoli zarządzania w postaci pojedynczego interfejsu administracyjnego.
	iii. Automatyzację zadań związanych z administracją zasobami środowiska wirtualnego.

t)	W przypadku ograniczeń prawnych dotyczących sposobu zakupu, wynikających z postanowień licencyjnych Producenta Oprogramowania, Dzierżawca wymaga zakupu przez Wydzierżawiającego wymaganych licencji na rzecz Dzierżawcy.

Tabela 5: Wirtualna zapora ogniowa następnej generacji (Next Generation FireWall)

	Wymagania ogólne:
	System zabezpieczeń firewall musi być dostarczony jako specjalizowane wirtualne urządzenie zabezpieczeń sieciowych (tzw. virtual appliance) do uruchomienia w środowisku VMware ESXi, VMware NSX lub Microsoft Hyper-V.
	System zabezpieczeń firewall musi zapewniać wewnętrzne wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie architektury systemu, tj. w/w moduły muszą pracować na różnych wirtualnych rdzeniach procesora przydzielonych przez środowisko wirtualizacyjne. Musi istnieć możliwość niezależnego od siebie restartowania modułu zarządzania i modułu przetwarzania ruchu sieciowego.
	System zabezpieczeń firewall musi umożliwiać działanie w następujących trybach pracy:
	rutera (tzn. w warstwie 3 modelu OSI),
	przełącznika (tzn. w warstwie 2 modelu OSI),
	w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA)
	w trybie pasywnego nasłuchu (sniffer).

	Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych. System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tablice routingu. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. System zabezpieczeń firewall musi umożliwiać pracę w modelu wysokiej dostępności poprzez pracę dwóch urządzeń w modelu failover. Wymagana jest praca firewalli w modelach Active-Standby i Active-Active.
	Wymagania dot. Platformy: System zabezpieczeń firewall musi obsługiwać co najmniej 4096 interfejsów logicznych i fizycznych. System zabezpieczeń firewall musi być wyposażony w co najmniej jeden dedykowany interfejs do zarządzania Out-of-Band z własną tablicą routingu. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać min. 4094 znaczników VLAN. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 8 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 4 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) System zabezpieczeń firewall musi obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń i umożliwiać zestawianie nie mniej niż 60 000 połączeń na sekundę. System zabezpieczeń firewall musi umożliwiać realizację połączeń VPN z przepustowością nie mniejszą niż 4 Gbps.

Podstawowe wymagania funkcjonalne:

System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

Polityka zabezpieczeń firewall musi uwzględniać

strefy bezpieczeństwa,

adresy IP klientów i serwerów,

protokoły i usługi sieciowe,

aplikacje,

kategorie URL,

użytkowników aplikacji,

reakcje zabezpieczeń,

rejestrowanie zdarzeń i alarmowanie

zarządzanie pasmem w sieci w oparciu o

priorytet,

pasmo gwarantowane,

pasmo maksymalne,

oznaczenia DiffServ

System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń musi blokować wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

	System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach UDP i TCP. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole, gdzie definiowane są aplikacje i oddzielne pole, gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Kontrola aplikacji musi być przeprowadzana w sposób umożliwiający potraktowanie informacji o niej jako atrybutu, a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce. System zabezpieczeń firewall musi wykrywać co najmniej 2 500 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antymalware, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

	System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta musi być traktowana jako stanowiąca automatyczne wyjątki od ogólnych reguł deszyfracji. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. System firewall musi automatycznie weryfikować spójność konfiguracji polityk bezpieczeństwa z punku widzenia kompletności użytych przez administratora sygnatur aplikacyjnych potrzebnych do prawidłowego działania polityki. Np. jeśli do prawidłowej obsługi dostępu do aplikacji „Facebook" potrzebne jest dodatkowo użycie aplikacji „SSL", a administrator nie uwzględni tej aplikacji w polityce, to system powinien ostrzec o tym fakcie administratora w momencie zatwierdzania nowej polityki. System firewall musi posiadać możliwość zastosowania jako kryteriów dopasowywania ruchu w regułach polityki firewall obiektów dynamicznych typu: listy adresów IP, listy nazw domen FQDN, listy URL. Zawartość list dynamicznych powyższych typów powinna być aktualizowana automatycznie ze wskazanych w definicji obiektu zewnętrznych źródeł, zgodnie z zadanym harmonogramem czasowym w przedziałach od 5 min. do 30 dni. Urządzenia posiadają możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Istnieje możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.
	Wymaganie dotyczące identyfikacji użytkowników: System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci

	System zabezpieczeń firewall musi zapewniać integrację z Active Directory, Ms Exchange, Citrix, LDAP serwerami Terminal Services Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet, gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w system zabezpieczeń firewall, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowania użytkowników. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku, gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
	Wymagania dot. warstwy sieci:

System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.

System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).

System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów.

Polityki definiujące powinny umożliwiać wykorzystanie

adresów źródłowych,

adresów docelowych,

użytkowników,

numerów portów usług

kategorie URL.

	System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
	Wymagania dotyczące zaawansowanych systemów ochrony: System firewall musi posiadać mechanizm blokujący możliwości wprowadzania przez użytkowników swoich poświadczeń domenowych (nazwa użytkownika, hasło) podczas dostępu do niezaufanych kategorii stron WWW. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW, który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.

System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).

System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).

System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

System zabezpieczeń firewall musi posiadać moduł antymalware lub antyspyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja antymalware lub antyspyware uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).

System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur antymalware lub antyspyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym . Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box". Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box". System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste

	adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
	Wymagania dotyczące zarządzania: Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).

	System zabezpieczeń firewall musi przechowywać logi i raporty. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie dopuszcza się, aby do tego celu konieczny był zakup zewnętrznych urządzeń, oprogramowania ani licencji. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach filtrowaniu stron www. System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

	System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów programowych systemu zabezpieczeń oraz łączy sieciowych.
	Wymagania dotyczące wsparcia technicznego: Pomoc techniczna musi być świadczona w języku polskim poprzez centrum kompetencyjne zlokalizowane w Polsce. Szkolenia dotyczące konfiguracji i obsługi systemu zabezpieczeń firewall muszą być dostępne i świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym zlokalizowanym w Polsce.
	Wymagania dotyczące dostaw: Dzierżawca wymaga dostawy 1 urządzenia opisanego powyżej z: Serwisem 3 letnim obejmującym usuwanie usterek w oprogramowaniu systemowym oraz aktualizacje tego oprogramowania przez okres 3 lat Subskrypcją na antywirus (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AV) na okres 3 lat Subskrypcją na antyspyware (lub antymalware jeżeli dla urządzenia nie jest dostępna licencja AS) na okres 3 lat Subskrypcją na IPS na okres 3 lat Dzierżawca wymaga możliwości rozbudowy o następujące subskrypcje/licencje jednakże nie wymaga ich dostawy w ramach niniejszego postępowania przetargowego Subskrypcją na URL Filtering

Subskrypcja na Remote Access VPN oraz kontrolę stanu stacji Subskrypcja umożliwiające przesyłanie plików do chmurowego/lokalnego sandboxa

ZAŁĄCZNIK NR 3 DO SIWZ (po zmianach z dnia 6.06.2018 r.)

ISTOTNE POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO UMOWY NR .....

zawarta w dniu ..... w Warszawie, dalej zwaną „Umową" pomiędzy :

Lotniczym Pogotowiem Ratunkowym z siedzibą w Warszawie przy ul. Księżycowej 5, kod 01-934 Warszawa wpisanym do Krajowego Rejestru Sądowego Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji i Publicznych Zakładów Opieki Zdrowotnej pod nr 0000144355, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, REGON 016321074, NIP 522-25-48-391
zwanym dalej **Dzierżawcą**
reprezentowanym przez: Dyrektora - Roberta Gałązkowskiego,

a

...
z siedzibą w ..., ul. ..., kod ... ..., wpisaną do ...
zwanym dalej **Wydzierżawiającym,**
reprezentowaną przez ...,

zwanymi dalej łącznie **Stronami.**

Mając na uwadze kończącą się umowę dzierżawy na macierz z przełącznikami sieciowymi, serwerami wirtualizacyjnymi oraz osprzętem, Dzierżawca celem zapewnienia działalności statutowej zawiera niniejszą umowę w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie: przetargu nieograniczonego nr ZP/..... „....." Zgodnie z postanowieniami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jedn. Dz. U. Nr 113 poz. 759), Strony zawierają umowę następującej treści:

§ 1

1. Wydzierżawiający oddaje w dzierżawę Dzierżawcy celem używania i pobierania pożytków „System wirtualizacji serwerów" szczegółowo opisany w Opisie Przedmiotu Zamówienia (stanowiącym załącznik nr 1 do Umowy) zgodnie ze złożoną przez Wydzierżawiającego ofertą stanowiącą załącznik nr 2 do Umowy, zwany dalej „przedmiotem dzierżawy".
2. Umowa zostaje zawarta na czas określony 36 miesięcy, liczonych od dnia zawarcia Umowy do ostatniego dnia miesiąca, w którym nastąpi zapłata ostatniej 35 - raty dzierżawnej.
3. Przedmiot dzierżawy pozostanie własnością Wydzierżawiającego przez cały czas trwania Umowy.

§ 2

Wydzierżawiający oświadcza, iż przedmiot dzierżawy jest:

a) fabrycznie nowy, nigdy wcześniej nie używany;
b) pochodzi z autoryzowanego kanału dystrybucji producenta na rynek polski;
c) posiada wszelkie parametry techniczne oraz funkcje niezbędne do korzystania z niego zgodnie z jego przeznaczeniem;

d) nie jest przedmiotem jakichkolwiek ograniczonych praw rzeczowych ustanowionych na rzecz osób trzecich, jak również nie jest przedmiotem jakichkolwiek postępowań sądowych, administracyjnych, czy też sądowo-administracyjnych, których konsekwencją jest (mogłoby być) ograniczenie czy też wyłączenie prawa Wydzierżawiającego do rozporządzania przedmiotem dzierżawy.

§ 3

1. Wydzierżawiający zobowiązany jest do dostarczenia przedmiotu dzierżawy na własny koszt i ryzyko do siedziby Dzierżawcy w stanie kompletnym, przez który Strony rozumieją stan gwarantujący użytkowanie przedmiotu dzierżawy zgodnie z jego przeznaczeniem, wraz z dokumentacją wymienioną w § 4 ust. 1.
2. Wydzierżawiający powiadomi pocztą elektroniczną Dzierżawcę na adres informatyk@lpr.com.pl o gotowości w dostarczeniu przedmiotu dzierżawy i w ten sam sposób ustali z Dzierżawcą termin dostawy.
3. Dostarczenie przedmiotu dzierżawy przez Wydzierżawiającego do siedziby Dzierżawcy nastąpi w terminie do 4 tygodni od daty zawarcia umowy.
4. Wydzierżawiający zobowiązuje się do instalacji na własny koszt przedmiotu dzierżawy w dniu jego dostawy oraz w miejscu wskazanym przez Dzierżawcę. Dostawa i instalacja przedmiotu dzierżawy zostanie potwierdzona protokołem dostawy.
5. Wydzierżawiający zobowiązuje się w terminie do 7 dni od instalacji przedmiotu dzierżawy, na wykonanie wdrożenia zgodnie z Opisem Przedmiotu Zamówienia, polegającym na uruchomieniu przedmiotu dzierżawy, w tym w szczególności między innymi na stworzeniu infrastruktury teletechnicznej oraz migracji serwerowych systemów operacyjnych z obecnie wykorzystywanej macierzy przez Dzierżawcę. Wykonanie prac zostanie potwierdzone protokołem zdawczo - odbiorczym.

§ 4

1. Wydzierżawiający zobowiązany jest dostarczyć w dniu odbioru wdrożenia wszystkie wymagane instrukcje obsługi w języku polskim, dokumentację techniczną, oraz harmonogram finansowy określający terminy i wysokość wszystkich opłat jakie poniesie Dzierżawca z tytułu realizacji Umowy, stanowiący załącznik nr 3 do Umowy, zwanym dalej Harmonogramem finansowym.
2. Dzierżawca zobowiązany jest do odbioru przedmiotu dzierżawy oraz do zbadania jego stanu technicznego w terminie do 7 dni liczonych od podpisania protokołu dostawy, bez zastrzeżeń.
3. Odbiór przedmiotu dzierżawy zostanie potwierdzony przez strony w protokole zdawczo -odbiorczym.
4. Protokół zdawczo-odbiorczy musi zawierać:
   a) potwierdzenie realizacji dostawy zgodnie z Umową, ofertą Wydzierżawiającego i Opisem Przedmiotu Zamówienia,
   b) wartość i datę dostawy,
   c) informację o producencie sprzętu,
   d) informację o przekazaniu instrukcji producenta,
   e) informację dotyczącą warunków serwisowania sprzętu i zaleceń w zakresie serwisu i przeglądów.

§ 5

1. Całkowita wartość Umowy, określona w ofercie Wydzierżawiającego, stanowiąca jego wynagrodzenie ryczałtowe, wynosi ..... zł netto, do ceny netto zostanie

doliczony podatek VAT w wysokości ..... zł, co stanowi łącznie z podatkiem VAT wynagrodzenie ryczałtowe brutto w wysokości ..... zł.

2. Wynagrodzenie, określone w ust 1 będzie płatne Wydzierżawiającemu zgodnie z następującymi opłatami:
   a) opłata wstępna w wysokości 25 % wartości przedmiotu dzierżawy określonego w ofercie Wydzierżawiającego, stanowiąca pierwsza ratę dzierżawy tj. ..... zł netto,
   b) kolejne 35 równych, miesięcznych rat dzierżawnych w łącznej wysokości ..... zł netto,

   płatne zgodnie z terminami przewidzianymi w Harmonogramie finansowym.
3. Kwota określona w ust. 1 obejmuje wszystkie opłaty określone w ust. 2 oraz koszty dostawy przedmiotu dzierżawy do Dzierżawcy.
4. Wydzierżawiający, w przypadku zwłoki z zapłatą poszczególnych rat dzierżawnych przez Dzierżawcę, może dochodzić od niego ustawowych odsetek za opóźnienie .
5. Opłata wstępna zostanie uiszczona przez Dzierżawcę na rachunek bankowy Wydzierżawiającego w terminie 7 dni od dnia zawarcia Umowy na podstawie faktury VAT wystawionej przez Wydzierżawiającego.
6. Pierwsza rata dzierżawy zostanie uiszczona przez Dzierżawcę na rachunek bankowy Wydzierżawiającego prowadzony w Banku o nr ..... w terminie 30 dni liczonych od podpisania przez strony protokołu zdawczo-odbiorczego przedmiotu dzierżawy bez zastrzeżeń i dostarczenia Dzierżawcy prawidłowo wystawionej faktury VAT.
7. Druga i kolejne raty dzierżawne będą płatne do 25 dnia każdego kolejnego miesiąca począwszy od miesiąca następującego po miesiącu płatności pierwszej raty, z dołu na podstawie prawidłowo wystawianych comiesięcznie przez Wydzierżawiającego faktur VAT, w wysokości ustalonej zgodnie z § 5 ust. 2 lit. b Umowy i wynikającej z Harmonogramu finansowego.
8. Wszelkie płatności przewidziane w Umowie będą dokonywane na rachunek bankowy Wydzierżawiającego wskazany na fakturze VAT.
9. Za dzień dokonania wszelkich płatności wynikających z Umowy uważa się dzień uznania rachunku bankowego Dzierżawcę.
10. W przypadku zaistnienia sytuacji określonej §13 ust 2 lit. b) kolejne raty będą w wysokości nie wyższej niż średnia miesięczna rata.

§ 6

1. Jako zabezpieczenie spłaty swoich zobowiązań Dzierżawca w dniu zawarcia Umowy wystawi weksel in blanco wraz z deklaracją wekslową do kwoty określonej w § 5 ust. 1 Umowy, według wzoru weksla i deklaracji wekslowej Wydzierżawiającego.
2. Wydzierżawiający uprawniony jest do wypełnienia weksla in blanco zgodnie z deklaracją wekslową.
3. Wydzierżawiający zobowiązany jest zwrócić Dzierżawcy weksel in blanco wraz z deklaracją wekslową niezwłocznie po wygaśnięcia Umowy lub w przypadku zaistnienia okoliczności określonych w § 10 Umowy.

§ 7

1. Wydzierżawiający w ramach gwarancji i rękojmi dostarczy na przedmiot dzierżawy pakiety rozszerzonego wsparcia producenta na łączny okres minimum 36 miesięcy licząc od chwili produkcyjnego uruchomienia środowiska, potwierdzonego protokołem zdawczo - odbiorczym. Szczegółowe warunki takiego wsparcia są określone na stronach internetowych producentów sprzętu. Rozszerzone wsparcie serwisowe

producentów urządzeń („urządzenie") wchodzących w przedmiotu dzierżawy (serwis producenta) wraz z oprogramowaniem ma zapewnić:

a) udostępnienia Dzierżawcy co najmniej jednego, dostępnego całodobowo numeru telefonu serwisowego (hot-line) do zgłaszania awarii, uwag, próśb i pytań w języku polskim, a także elektronicznego systemu zgłoszeń, pozwalającego Dzierżawcy na samodzielną analizę częstotliwości i czasów rozwiązania zgłoszeń oraz przeszukiwanie bazy wiedzy zbudowanej na podstawie historii poprzednich zgłoszeń,
b) realizacji zgłoszeń zgodnie z czasem reakcji (rozumianym jako rozpoczęcie komunikacji dedykowanego inżyniera Wydzierżawiającego z osobą zgłaszającą) na zgłoszenie na poziomie:
    - 30 minut dla awarii krytycznych, przez które rozumie się zatrzymanie przetwarzania albo brak dostępu do elementów usługowych środowiska (np. brak dostępu do zasobów dyskowych, brak dostępu do maszyn wirtualnych)
    - 2 godziny dla awarii zwykłych, przez które rozumie się zatrzymanie przetwarzania jednej ze składowych środowiska skutkujące brakiem redundancji (np. awaria jednej z macierzy, przełącznika SAN, serwera) lub nieprawidłowe zachowanie środowiska wirtualizacji (np. brak dostępu administracyjnego do serwerów, konsoli zarządzające środowiskiem wirtualizacji lub nieprawidłowe i nieprzewidziane zachowania hypervisorów lub maszyn wirtualnych)
    - 8 godzin dla konsultacji eksperckich – pomoc w rekonfiguracji i planowaniu rozwoju środowiska, odpowiedzi na pytania związane ze specyfiką produktów wchodzących w skład niniejszego projektu,
c) realizacji zgłoszeń zgodnie z czasem reakcji onsite (rozumianym jako przybycie inżyniera certyfikowanego w danej technologii na miejsce do siedziby Dzierżawcy) na zgłoszenia na poziomie:
    - 4 godzin dla awarii krytycznych
    - następnego dnia dla awarii zwykłych
d) bezpośredni dostęp do ekspertów technicznych producenta poprzez centrum pomocy technicznej producenta, obejmujący pomoc ekspertów technicznych producenta przy diagnostyce problemów związanych z funkcjonowaniem urządzeń i oprogramowania producenta, użytkowanych w infrastrukturze Zamawiającego,
e) dostarczenie /naprawę /wymianę urządzenia w czasie zgodnym z typem urządzenia,
f) dostęp do aktualizacji i poprawek oprogramowania dla urządzenia, objętego rozszerzonym wsparciem serwisowym producenta,
g) posiadanie pełnej kontroli nad zgłoszeniami serwisowymi dla urządzenia, objętego rozszerzonym wsparciem serwisowym producenta,
h) brak ograniczeń co do liczby zgłoszeń serwisowych dla urządzenia, objętego rozszerzonym wsparciem serwisowym producenta.

2. Wydzierżawiający zobowiązany jest dostarczyć dokument wystawiony przez producenta dostarczanego urządzenia, potwierdzający pochodzenie sprzętu z oficjalnego kanału dystrybucji producenta na terenie Polski z informacją o tym, że oferowane urządzenia są fabrycznie nowe i zostaną objęte serwisem producenta w Polsce.

§ 8

1. Dzierżawca ma prawo ingerować zgodnie ze swoją najlepszą wiedzą w konfigurację przedmiotu dzierżawy.

2. Dzierżawca ponosi opłaty i koszty związane z należytą eksploatacją przedmiotu dzierżawy, jak również opłaty i koszty związane z własnością i posiadaniem przedmiotu dzierżawy, w tym jego ubezpieczeniem.

§ 9

1. Za każdy dzień opóźnienia w realizacji terminów określonych w Umowie lub na jej podstawie Dzierżawca może żądać od Wydzierżawiającego zapłaty kary umownej w wysokości 0,1 % wartości brutto Umowy, określonej w § 5 ust. 1 Umowy, z tym jednak zastrzeżeniem, że łączna wysokość kar umownych należnych Dzierżawcy z tego tytułu nie może przekroczyć 20 % całkowitej wartości brutto Umowy, określonej w § 5 ust. 1 umowy.
2. W przypadku wystąpienia opóźnienia w realizacji terminów określonych w Umowie lub na jej podstawie skutkujących naliczeniem maksymalnych kar umownych tj. kar umownych w wysokości 20 % całkowitej wartości brutto Umowy, określonej w § 5 ust. 1 Umowy, Dzierżawca może rozwiązać umowę ze skutkiem natychmiastowym i dochodzić odszkodowania uzupełniającego na zasadach ogólnych.

§ 10

1. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, Dzierżawca może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
2. W przypadku, o którym mowa w ust. 1, Wydzierżawiający może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
3. Dzierżawca może odstąpić od Umowy w całości lub w części w przypadku, gdy:
   a) Wydzierżawiający opóźnia się z wydaniem przedmiotu dzierżawy o ponad 10 dni w stosunku do terminu określonego w § 3 ust.3,
   b) przedmiot dzierżawy nie spełnia warunków określonych w umowie i specyfikacji istotnych warunków zamówienia, a Wydzierżawiający nie dostarczył w dodatkowym terminie określonym przez Dzierżawcę przedmiotu dzierżawy spełniającego te kryteria,
   c) otwarcia likwidacji Wydzierżawiającego,
   d) zajęcia majątku Wydzierżawiającego w stopniu uniemożliwiającym mu wykonanie Umowy,
   e) utraty przez Wydzierżawiającego uprawnień niezbędnych do wykonania Umowy,
   f) termin dostawy przekroczy termin określony w §3 ust. 3.
4. Oświadczenie o odstąpieniu powinno nastąpić na piśmie w terminie 30 dni od zaistnienia okoliczności, o których mowa w ust. 3.
5. W przypadku odstąpienia przez Dzierżawcę od Umowy w całości z przyczyn określonych w ust. 3, Dzierżawca ma prawo obciążyć Wydzierżawiającego kwotą w wysokości 20% kwoty brutto określonej w § 5 ust. 1 Umowy.
6. W przypadku odstąpienia przez Dzierżawcę od Umowy w części z przyczyn określonych w ust. 3, Dzierżawca ma prawo obciążyć Wydzierżawiającego kwotą w wysokości 20% niezrealizowanej wartości brutto Umowy określonej w § 5 ust. 1 Umowy.

§ 11

1. Dzierżawca może wypowiedzieć Umowę z zachowaniem jednomiesięcznego okresu wypowiedzenia w przypadku nie wykonania lub nienależytego wykonywania przez Wydzierżawiającego obowiązków wynikających z umowy, jeżeli Wydzierżawiający po

uprzednim wezwaniu przez Dzierżawcę w dalszym ciągu nie wykonuje lub nienależycie wykonuje umowę.

2. Wydzierżawiający może wypowiedzieć Umowę z zachowaniem jednomiesięcznego okresu wypowiedzenia w przypadku gdy:
   a) Dzierżawca używa przedmiotu dzierżawy w sposób sprzeczny z jego przeznaczeniem lub właściwościami i nie zaprzestaje takich działań pomimo udzielenia mu pisemnego upomnienia przez Wydzierżawiającego,
   b) Dzierżawca dopuszcza się zwłoki z zapłatę jednej raty dzierżawnej i nie dokonuje płatności pomimo wezwania przez Wydzierżawiającego wysłanego listem poleconym za zwrotnym potwierdzeniem odbioru, wyznaczającego dodatkowy, 14 dniowy termin do zapłaty,
   c) Dzierżawca odda przedmiot dzierżawy osobie trzeciej do używania bez zgody Wydzierżawiającego,
   d) Dzierżawca istotnie naruszy inne postanowienia niniejszej Umowy.
3. W przypadku rażącego naruszania przez Wydzierżawiającego postanowień Umowy Dzierżawca może rozwiązać Umowę ze skutkiem natychmiastowym.
4. W przypadku wypowiedzenia lub rozwiązania Umowy zgodnie z niniejszym paragrafem Dzierżawca może obciążyć Wydzierżawiającego karą umowną w wysokości 20% wartości Umowy określonej w § 5 ust. 1 Umowy.

§ 12

1. W sytuacji obciążenia Wydzierżawiającego karą umowną Dzierżawca wystawi Wydzierżawiającemu notę obciążeniową z terminem płatności do 7 dni od daty jej otrzymania.
2. W przypadku powstania szkody przewyższającej wysokość kar umownych Strony mogą dochodzić odszkodowania przewyższającego wysokość zastrzeżonych kar umownych, na zasadach ogólnych.
3. Dzierżawca będzie zobowiązany do zwrotu przedmiotu dzierżawy w terminie do 30 dni od daty rozwiązania Umowy.
4. Przedmiot dzierżawy powinien zostać zwrócony Wydzierżawiającemu w stanie nie pogorszonym, przy czym Dzierżawca nie będzie ponosił odpowiedzialności za jego zużycie będące następstwem użytkowania w sposób odpowiadający właściwościom i przeznaczeniu rzeczy.

§ 13

1. Strony zgodnie z art. 144 ustawy Prawo zamówień publicznych ustalają, że zmiana Umowy może nastąpić według zasad i na warunkach określonych w ust 3.
2. Dzierżawca przewiduje możliwość dokonania istotnych zmiany Umowy w następujących sytuacjach:
   a) Zmiany terminu dostawy przedmiotu dzierżawy w przypadku dostawy sprzętu zastępczego celem zapewnienia działalności statutowej Dzierżawcy,
   b) Zmiany terminu i wynagrodzenia za przedmiot dzierżawy po zakończeniu umowy w przypadku dalszej potrzeby użytkowania przedmiotu dzierżawy przez Dzierżawcę, nie dłużej jednak jak o 6 miesięcy,
   c) obniżenie wartości za przedmiot dzierżawy przez Wydzierżawiającego może nastąpić w każdym czasie,
   d) nastąpiła zmiana stawki podatku VAT – cena netto nie ulegnie zmianie, nastąpi jedynie zmiana ceny brutto; Wydzierżawiający jest uprawniony do zmiany wysokości rat dzierżawnych w trakcie trwania Umowy dzierżawy tylko w

przypadku zmiany wysokości stawki podatku VAT w trakcie obowiązywania Umowy. Zmiana wysokości rat dzierżawnych wymaga aneksu do umowy.

e) zmiany w obowiązujących przepisach prawa mające wpływ na przedmiot i warunki Umowy oraz zmiana sytuacji prawnej lub faktycznej Wydzierżawiającego i/lub Dzierżawcę skutkująca nie możliwością realizacji przedmiotu dzierżawy.

§ 14

1. Umowa wchodzi w życie z dniem podpisania.
2. W sprawach nieuregulowanych umową będą miały zastosowanie w szczególności przepisy kodeksu cywilnego oraz ustawy prawo zamówień publicznych.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Spory wynikające z Umowy będą rozstrzygane przez Sąd właściwy dla miejsca siedziby Dzierżawcę.
5. Umowę sporządzono w czterech egzemplarzach, w tym trzy egzemplarze dla Dzierżawcę i jeden dla Wydzierżawiającego.
6. Integralną część Umowy stanowią:
   1) Załącznik nr 1: Opis przedmiotu zamówienia,
   2) Załącznik nr 2: Oferta Wykonawcy,
   3) Załącznik nr 3: Harmonogram finansowy.

.....	.....
DZIERŻAWCA	*WYDZIERŻAWIAJĄCY*

Z-ca DYREKTORA
ds. Administracyjnych/Główny Księgowy
Lotnicze Pogotowie Ratunkowe
Paweł Kamiński

RADCA PRAWNY
Szymon Barusiński
KL/1075