Kraków, dnia 13.11.2020 r.

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Przetarg nieograniczony o wartości wyrażonej w złotych polskich

poniżej równowartości 214 000 euro

**Dostawa sprzętu i oprogramowania informatycznego IV**

Zamawiający:

Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny

30-418 Kraków, ul. Zakopiańska 73

ZATWIERDZAM:

# Nazwa oraz adres Zamawiającego

Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny

30-418 Kraków, ul. Zakopiańska 73

tel. (12) 26 18 324/111, faks (12) 26 60 870

NIP 675-000-00-88 REGON 387116932

Adres strony internetowej: https://kit.lukasiewicz.gov.pl/

Adres poczty elektronicznej: sekretariat@kit.lukasiewicz.gov.pl

## Tryb udzielenia zamówienia

Postępowanie jest prowadzone w trybie przetargu nieograniczonego o wartości wyrażonej w złotych polskich poniżej równowartości 214 000,00 euro.

*Gdziekolwiek w niniejszej specyfikacji przywołana jest ustawa lub przepis bez dalszego uszczegółowienia to należy przez to rozumieć Ustawę Prawo Zamówień Publicznych.*

# Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa sprzętu i oprogramowania informatycznego, w tym:

Część I - Zakup i dostawa dwóch klastrów urządzeń klasy UTM

Część II - Zakup i dostawa macierzy flash

Część III - Przedłużenie usługi wsparcia technicznego producenta na kolejny rok dla infrastruktury macierzy dyskowych posiadanych przez Zamawiającego

Część IV - Zakup i dostawa dysku zewnętrznego

Część V - Dostawa oprogramowania serwerowego Windows Server Standard Core 2 SL lub równoważnego wraz z licencjami dostępowymi Windows Server User CAL lub równoważnymi

Część VI - Zakup oprogramowania do obróbki graficznej CorelDRAW Graphics Suite 2020 lub równoważnego

Część VII –  Zwiększenie  o 150 stanowisk  licencji  na posiadane przez Zamawiającego  oprogramowanie antywirusowe ESET Endpoint Antivirus Suite

Część I: CPV: 32420000-3

Część II: CPV: 30233141-1

Część III: CPV: 71356300-1

Część IV: CPV: 30234000-8, 30234100-9

Część V: CPV: 48214000-1

Część VI: CPV: 48322000-1

Część VII: CPV: 48760000-3, 48761000-0

Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 3 do SIWZ,

Gdziekolwiek w Specyfikacji Istotnych Warunków Zamówienia przywołane są normy, lub nazwy własne lub znaki towarowe lub patenty lub pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty dostarczane przez konkretnego wykonawcę Zamawiający dopuszcza rozwiązania równoważne.

# Termin wykonania zamówienia

Część I: Termin dostawy: 3 tygodnie

Część II: Termin dostawy: 3 tygodnie

Część III: Termin dostawy: 7 dni

Część IV: Termin dostawy: 7 dni

Część V: Termin dostawy: 7 dni

Część VI: Termin dostawy: 7 dni

Część VII: Termin dostawy: 7 dni

- od daty zawarcia umowy

# Warunki udziału w postępowaniu

Zamawiający nie stawia warunków udziału w postępowaniu.

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 24 ust. 1 ustawy Pzp. Podstawy wykluczenia podane w punkcie poniżej.

# 6. Podstawy do wykluczenia Wykonawcy z postępowania

Podstawy wykluczenia Wykonawcy zostały podane w art 24 ust. 1 ustawy Prawo zamówień publicznych. Art 24 ust 1 ustawy Prawo zamówień publicznych stanowi:

Z postępowania o udzielenie zamówienia wyklucza się:

12) wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie został zaproszony do negocjacji lub złożenia ofert wstępnych albo ofert, lub nie wykazał braku podstaw wykluczenia;

13) 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. z 2016 r. poz. 1137, 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, 1170 i 1171 oraz z 2017 r. poz. 60 i 1051),

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);

14) 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 13;

15) 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;

16) 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, zwane dalej „kryteriami selekcji”, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów;

17) 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;

18) wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;

19) 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;

20) 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;

21) 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 2016 r. poz. 1541, oraz z 2017 r. poz. 724 i 933);

22) wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne;

23) 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 2017 r. poz. 229, 1089 i 1132), 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.

Zgodnie z art. 24 ust 7 ustawy Prawo zamówień publicznych wykluczenie wykonawcy następuje:

1) w przypadkach, o których mowa w ust. 1 pkt 13 lit. a–c i pkt 14, gdy osoba, o której mowa w tych przepisach została skazana za przestępstwo wymienione w ust. 1 pkt 13 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. 1 pkt 13 lit. d i pkt 14, gdy osoba, o której mowa w tych przepisach, została skazana za przestępstwo wymienione w ust. 1 pkt 13 lit. d,

b) w ust. 1 pkt 15,

c) ~~w ust. 5 pkt 5–7~~

– 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. 1 pkt 18 i 20 lub ~~ust. 5 pkt 2 i 4~~, jeżeli nie upłynęły 3 lata od dnia zaistnienia zdarzenia będącego podstawą wykluczenia;

4) w przypadku, o którym mowa w ust. 1 pkt 21, jeżeli nie upłynął okres, na jaki został prawomocnie orzeczony zakaz ubiegania się o zamówienia publiczne;

5) w przypadku, o którym mowa w ust. 1 pkt 22, jeżeli nie upłynął okres obowiązywania zakazu ubiegania się o zamówienia publiczne.

Ponadto zgodnie z art 24 ust 8,9,10,11 oraz 12 ustawy Prawo zamówień publicznych procedura wykluczenia Wykonawcy przebiega następująco:

- Wykonawca, który podlega wykluczeniu na podstawie ust. 1 pkt 13 i 14 oraz 16–20 l~~ub ust. 5,~~ 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.

- Wykonawca nie podlega wykluczeniu, jeżeli zamawiający, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, uzna za wystarczające dowody przedstawione na podstawie ust. 8.

- W przypadkach, o których mowa w ust. 1 pkt 19, przed wykluczeniem wykonawcy, zamawiający zapewnia temu wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji. Zamawiający wskazuje w protokole sposób zapewnienia konkurencji.

- Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5, przekazuje zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w ust. 1 pkt 23. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

- Zamawiający może wykluczyć wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

Zamawiający zastrzega sobie prawo do tego, aby najpierw dokonać oceny ofert, a następnie zbadać, czy wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

# 7. Wykaz oświadczeń lub dokumentów potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia a także spełnianie przez oferowany przedmiot zamówienia wymagań określonych przez Zamawiającego

Na potwierdzenie braku podstaw do wykluczenia z postępowania Zamawiający żąda od Wykonawcy przedłożenia wraz z ofertą oświadczenia o którym mowa w pkt. 8 SIWZ.

**I.**

Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 przekazuje zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art 24 ust. 1 pkt 23. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

Treść art 86 ust 5 od którego liczony jest 3 dniowy termin o którym mowa w zdaniu powyżej brzmi:

Niezwłocznie po otwarciu ofert zamawiający zamieszcza na stronie internetowej informacje dotyczące:

1) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;

2) firm oraz adresów wykonawców, którzy złożyli oferty w terminie;

3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

# 8. Kształt oferty oraz wymagania w zakresie oświadczeń i dokumentów które Wykonawcy powinni złożyć wraz z ofertą

Zamawiający wymaga od Wykonawcy złożenia:

a) pełnomocnictwa do podpisania oferty i składania ewentualnych wyjaśnień, jeżeli osobą podpisującą nie jest osoba upoważniona na podstawie wypisu z Krajowego Rejestru Sądowego lub zaświadczenia o wpisie do centralnej ewidencji i informacji o działalności gospodarczej. Jeżeli dołączone do oferty ww. pełnomocnictwo będzie w formie kopii, Zamawiający wymaga, aby jego zgodność z oryginałem poświadczyła osoba wymieniona w rejestrze, która jest wskazana, jako upoważniona do reprezentowania Wykonawcy lub notariusz,

b) oświadczenia Wykonawcy zgodnie z załącznikiem nr **1**,

c) wypełnionego formularza ofertowego wg załącznika nr **4**.

Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W powyższym przypadku wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców, którzy wspólnie ubiegają się o udzielenie zamówienia. Jeżeli oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zostanie wybrana, zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych wykonawców.

W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, jednolity dokument lub oświadczenie składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu lub kryteriów selekcji oraz brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu lub kryteriów selekcji oraz brak podstaw wykluczenia.

Wykonawca może wykorzystać w jednolitym dokumencie nadal aktualne informacje zawarte w innym jednolitym dokumencie złożonym w odrębnym postępowaniu o udzielenie zamówienia.

# 9. Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń lub dokumentów

1. Zamawiający będzie porozumiewał się z Wykonawcami wyłącznie pisemnie. Informacja o rozstrzygnięciu postępowania może być przesłana również drogą mailową lub faxu. Korespondencję należy kierować na adres zamawiającego: **Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny , ul. Zakopiańska 73, 30-418 Kraków**

2. We wszelkich kontaktach z Zamawiającym Wykonawcy powinni powoływać się na numer oraz nazwę procedury przetargowej: **ZP/12/20 Dostawa sprzętu i oprogramowania informatycznego IV**

3. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami w sprawie przetargu jest:

- w sprawach formalnych - Marek Dziewit – tel. 693 289 533

- w sprawach merytorycznych – Elżbieta Tomczyk – tel. 48 12 261 81 87

# 10. Wymagania dotyczące wadium

Zamawiający nie wymaga wniesienia wadium.

# 11. Termin związania ofertą

Wykonawca związany jest ofertą przez okres 30 dni licząc od ostatecznego terminu składania ofert.

# 12. Opis sposobu przygotowania ofert oraz dokumentów i oświadczeń wymaganych w SIWZ

1. Oferta powinna zawierać wszystkie wymagane w pkt 8 niniejszej SIWZ oświadczenia i dokumenty, bez dokonywania w ich treści jakichkolwiek zastrzeżeń lub zmian ze strony Wykonawcy.
2. Oferta powinna być:
   * sporządzona na podstawie załączników niniejszej SIWZ.
   * napisana w języku polskim na maszynie, komputerze lub inną trwałą techniką.

- złożona w zapieczętowanej kopercie oznaczonej nazwą i adresem Wykonawcy oraz napisem: **„ZP/12/20 Dostawa sprzętu i oprogramowania informatycznego IV**

**Nie otwierać przed dniem 25.11.2020 r. przed godziną 9:30”.**

1. Wszelkie poprawki lub zmiany w tekście oferty muszą być parafowane i datowane własnoręcznie przez osobę podpisująca ofertę.
2. Każdy z Wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
3. Ceny oferty muszą zawierać wszystkie koszty jakie musi ponieść Wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
4. Oświadczenia, o których mowa w SIWZ dotyczące wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a ustawy Prawo zamówień publicznych oraz dotyczące podwykonawców, składane są w oryginale. Pozostałe dokumenty, inne niż oświadczenia, o których mowa w zdaniu powyżej, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem. 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. Dokumenty i oświadczenia składane przez Wykonawcę powinny być w języku polskim  
   chyba, że w SIWZ dopuszczono inaczej. W przypadku  załączenia dokumentów sporządzonych w innym języku niż dopuszczony, Wykonawca zobowiązany jest załączyć tłumaczenie na język polski.

Wprowadzanie zmian do oferty i jej wycofanie.

1. Wykonawca może wprowadzić zmiany lub wycofać złożoną ofertę przed upływem terminu składania ofert.
2. Powiadomienie o wprowadzeniu zmian lub wycofaniu oferty winno zostać złożone w sposób i formie przewidzianej dla oferty, z tym, że koperta powinna być dodatkowo oznaczona dopiskiem “zmiana" lub “wycofanie".

# 13. Miejsce oraz termin składania i otwarcia ofert

1. Ofertę należy złożyć w siedzibie Zamawiającego: **Sieć Badawcza Łukasiewicz –** **Krakowski Instytut Technologiczny, ul. Zakopiańska 73, 30-418 Kraków, Budynku „BLT” (wejście od strony ul. Zbrojarzy), II piętro – Sekretariat Dyrektora, w dni robocze, w godzinach: 8.00 – 16.00 do dnia: 25.11.2020 r. do godziny 9:00.**

Oferty złożone po upływie terminu składania ofert zostaną odesłane bez otwierania.

1. 2. Publiczne otwarcie ofert nastąpi w siedzibie Zamawiającego **w dniu 25.11.2020 r. o godz. 9:30 w Budynku „BLT” I piętro, sala konferencyjna, Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny, Kraków ul. Zakopiańska 73.**

# 14. Opis sposobu obliczania ceny

1. Wykonawca zobowiązany jest do podania cen w sposób określony w **załączniku nr 4**.

# 15. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert.

Zamawiający przy wyborze ofert będzie kierował się kryteriami podanymi w poniższej tabeli.

Część I - VII :

|  |  |  |  |
| --- | --- | --- | --- |
| ***L.p.*** | **Kryterium** | ***Znaczenie procentowe kryterium (Rj)*** | ***Maksymalna ilość punktów, jakie może otrzymać oferta za dane kryterium*** |
| 1. | Cena | C = 100% | 100 punktów |

# 17.2 Sposób oceny ofert ( dla wszystkich części )

Zamawiający wybierze ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w SIWZ. Za najkorzystniejszą uznana zostanie ta z ocenianych ofert, która uzyska maksymalną ocenę punktową (**LP**) wg poniższego wzoru.

Dla powyższych kryteriów oceny ofert, Zamawiający będzie obliczał wartość punktową oferty (zaokrągloną do dwóch miejsc po przecinku) w oparciu o następujący wzór:

**Część I - VII**

**C = R1 x Cmin / Cb**

**Cmin – cena oferty najtańszej**

**Cb – cena oferty badanej**

**R1 – znaczenie procentowe kryterium Cena**

**UWAGA:** „Jeżeli w postępowaniu złożono ofertę, której wybór prowadzi do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy 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”.

# 16. Warunki umowy w sprawie zamówienia publicznego

1. Zamawiający wymaga, aby Wykonawca zawarł umowę w sprawie zamówienia publicznego wg wzoru stanowiącego załącznik nr **2** do SIWZ.

2. Zamawiający prześle umowę Wykonawcy, którego oferta została wybrana za najkorzystniejszą albo zaprosi go do swojej siedziby, celem podpisania umowy.

# 17. Wymagania dotyczące zabezpieczenia należytego wykonania umowy

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

# 18. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia

Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której zamawiający jest zobowiązany na podstawie ustawy.

Odwołanie przysługuje wyłącznie wobec czynności:

1) wyboru trybu negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę;

2) określenia warunków udziału w postępowaniu;

3) wykluczenia odwołującego z postępowania o udzielenie zamówienia;

4) odrzucenia oferty odwołującego;

5) opisu przedmiotu zamówienia;

6) wyboru najkorzystniejszej oferty.

Odwołanie powinno wskazywać czynność lub zaniechanie czynności zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.

Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej albo w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.

Odwołujący przesyła kopię odwołania zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia przy użyciu środków komunikacji elektronicznej.

Odwołanie wnosi się w terminie 5 dni od dnia przesłania informacji o czynności zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane w sposób określony w art. 180 ust. 5 zdanie drugie albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób.

Odwołanie wobec treści ogłoszenia o zamówieniu, a jeżeli postępowanie jest prowadzone w trybie przetargu nieograniczonego, także wobec postanowień specyfikacji istotnych warunków zamówienia, wnosi się w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub specyfikacji istotnych warunków zamówienia na stronie internetowej.

Odwołanie wobec czynności innych niż określone powyżej wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

Zamawiający przesyła niezwłocznie, nie później niż w terminie 2 dni od dnia otrzymania, kopię odwołania innym wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli odwołanie dotyczy treści ogłoszenia o zamówieniu lub postanowień specyfikacji istotnych warunków zamówienia, zamieszcza ją również na stronie internetowej, na której jest zamieszczone ogłoszenie o zamówieniu lub jest udostępniana specyfikacja, wzywając wykonawców do przystąpienia do postępowania odwoławczego.

Wykonawca może zgłosić przystąpienie do postępowania odwoławczego w terminie 3 dni od dnia otrzymania kopii odwołania, wskazując stronę, do której przystępuje, i interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje. Zgłoszenie przystąpienia doręcza się Prezesowi Izby w postaci papierowej albo elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, a jego kopię przesyła się zamawiającemu oraz wykonawcy wnoszącemu odwołanie.

Wykonawcy, którzy przystąpili do postępowania odwoławczego, stają się uczestnikami postępowania odwoławczego, jeżeli mają interes w tym, aby odwołanie zostało rozstrzygnięte na korzyść jednej ze stron.

Zamawiający lub odwołujący może zgłosić opozycję przeciw przystąpieniu innego wykonawcy nie później niż do czasu otwarcia rozprawy. Izba uwzględnia opozycję, jeżeli zgłaszający opozycję uprawdopodobni, że wykonawca nie ma interesu w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystąpił; w przeciwnym razie Izba oddala opozycję. Postanowienie o uwzględnieniu albo oddaleniu opozycji Izba może wydać na posiedzeniu niejawnym. Na postanowienie o uwzględnieniu albo oddaleniu opozycji nie przysługuje skarga.

Odwołanie podlega rozpoznaniu, jeżeli:

- nie zawiera braków formalnych;

- uiszczono wpis.

Wpis uiszcza się najpóźniej do dnia upływu terminu do wniesienia odwołania, a dowód jego uiszczenia dołącza się do odwołania.

# 19. Opis części zamówienia

Zamawiający dopuszcza składania ofert częściowych na jeden lub większą liczbę części opisanych w załącznikach do SIWZ. Zamawiający nie przewiduje maksymalnej liczby części, na które może być udzielone zamówienie jednemu wykonawcy

# 20. Maksymalna liczba wykonawców, z którymi zamawiający zawrze umowę ramową.

Nie dotyczy.

# 21. Informację o przewidywanych zamówieniach, o których mowa w art. 67 ust. 1 pkt 6 i 7 lub art. 134 ust. 6 pkt 3, jeżeli zamawiający przewiduje udzielenie takich zamówień

Zamawiający nie przewiduje zamówienia uzupełniającego, o których mowa w art. 67 ust. 1 pkt 6,7.

# 22. Opis sposobu przedstawiania ofert wariantowych oraz minimalne warunki, jakim muszą odpowiadać oferty wariantowe wraz z wybranymi kryteriami oceny.

Zamawiający nie dopuszcza składania ofert wariantowych.

# 23. Informacje dotyczące walut obcych w jakich mogą być prowadzone rozliczenia między Zamawiającym a Wykonawcą

Zamawiający nie dopuszcza możliwości rozliczenia z Wykonawcą w obcych walutach. Rozliczenia nastąpią w złotych polskich.

# 24. Aukcja elektroniczna

Zamawiający nie przewiduje aukcji elektronicznej.

# 25. Załączniki

1. Załącznik nr 1 – Oświadczenie Wykonawcy w zakresie niepodlegania wykluczeniu z

postępowania

2. Załącznik nr 1a - Oświadczenie Wykonawcy o przynależności albo braku przynależności do tej samej grupy kapitałowej

3.Załącznik nr 2 – Wzór umowy

4. Załącznik nr 3 – Opis przedmiotu zamówienia

5. Załącznik nr 4 – Formularz ofertowy

**26.Informacje i zasady przetwarzania danych osobowych przez Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny w Krakowie.**

Mając na uwadze zapisy art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, zwanym dalej „RODO”, poniżej podajemy informacje i zasady przetwarzania danych osobowych przez Instytut Odlewnictwa w Krakowie.

**Administrator danych**

Administratorem Pani/Pana (Wykonawcy) danych osobowych jest **Sieć Badawcza Łukasiewicz –** **Krakowski** **Instytut Technologiczny** w Krakowie (zwany dalej: Instytut lub Zamawiający) z siedzibą ul. Zakopiańska 73 30-418 Kraków, adres e-mail: sekretariat@kit.lukasiewicz.gov.pl nr tel.: **12 26 18 324**

**Inspektor Ochrony Danych**

We wszelkich sprawach dotyczących przetwarzania danych osobowych przez Instytut można kontaktować się   
z wyznaczonym w tym celu Inspektorem Ochrony Danych, adres email: daneosobowe@kit.lukasiewicz.gov.pl lub osobiście w siedzibie Instytutu.

**Cel przetwarzania danych osobowych i podstawa prawna przetwarzania danych:**

Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w związku z przepisami ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp" w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn.: **ZP/12/20 Dostawa sprzętu i oprogramowania informatycznego IV**

- znak sprawy: **ZP/12/20** prowadzonym w trybie przetargu nieograniczonego

**Odbiorcy danych**

Odbiorcami Państwa danych osobowych są lub mogą być:

* 1. osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy Pzp;
  2. podmioty serwisujące urządzenia Instytutu za pośrednictwem, których przetwarzane są Państwa dane osobowe;
  3. podmioty dostarczające i utrzymujące oprogramowanie wykorzystywane w celu przetwarzania danych osobowych Wykonawców, osób reprezentujących i pracowników Wykonawcy;
  4. podmioty świadczące na rzecz Instytutu usługi niezbędne do ewentualnego wykonania zawieranej z Państwem umowy – jeżeli zawarta z Państwem umowa wymaga ich udziału np. firmy kurierskie za pośrednictwem, których może być prowadzona z Państwem korespondencja.
  5. podmioty, którym przekazuje się dokumentację dla celów niszczenia po zakończonym okresie przechowywania;

Pani/Pana dane osobowe nie będą przekazywane do państw znajdujących się poza Europejskim Obszarem Gospodarczym i nie będą przekazywane do organizacji międzynarodowych.

**Okres, przez który dane będą przetwarzane**

Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy.

**Realizacja praw osób, których dane dotyczą**

Posiada Pani/Pan:

* prawo dostępu do danych osobowych Pani/Pana dotyczących (na podstawie art. 15 RODO);
* prawo do sprostowania Pani/Pana danych osobowych (na podstawie art. 16 RODO)\*;
* prawo żądania (na podstawie art. 18 RODO) od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO\*\*;
* prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2 00-193 Warszawa w przypadku uznania, że przetwarzanie przez Instytut Pani/Pana danych osobowych narusza przepisy RODO.

W celu wykonania praw wymienionych powyżej należy skierować żądanie na adres email: daneosobowe@kit.lukasiewicz.gov.pl, pisemnie na adres siedziby Instytutu lub osobiście w siedzibie Instytutu. Przed realizacją Państwa uprawnień Instytut musi potwierdzić Państwa tożsamość w sposób indywidualnie dostosowany do danego żądania.

Nie przysługuje Pani/Panu:

* w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
* prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
* na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

**Informacja o wymogu podania danych**

Obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego. Konsekwencje niepodania określonych danych wynikają z ustawy Pzp.

**Decyzje podejmowane w sposób zautomatyzowany**

Instytut nie będzie stosował wobec Pani/Pana zautomatyzowanego podejmowania decyzji, w tym profilowania.

Wyjaśnienie:

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

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

ZATWIERDZAM

**Załącznik nr 1**

**Zamawiający:**

**Sieć Badawcza Łukasiewicz**

**- Krakowski Instytut Technologiczny**

**30-418 Kraków, ul. Zakopiańska 73**

**Wykonawca:**

………………..………………………………………

*(pełna nazwa/firma)*

………………..………………………………………

*(adres)*

………………..………………………………………

*tel./fax)*

*.............................................................*

*w zależności od podmiotu: NIP/PESEL,KRS/CEiDG)*

reprezentowany przez:

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

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

**Oświadczenie Wykonawcy**

**składane na podstawie art. 25 a ust. 1 ustawy z dnia 29 stycznia 2004 r.**

**Prawo zamówień publicznych (dalej jako: ustawa Pzp),**

**DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA ORAZ SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU**

Na potrzeby postępowania o udzielenie zamówienia publicznego  
pn. ………………………………………………………………….…………. *(nazwa postępowania)*, prowadzonego przez **Sieć Badawczą Łukasiewicz –** **Krakowski Instytut Technologiczny**oświadczam, co następuje:

**OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:**

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie   
   art. 24 ust 1 pkt 12-22 ustawy Pzp.

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

…………………………………………

*(podpis)*

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. …………. ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze: …………………………….……………………………..

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

…………………………………………

*(podpis)*

**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)*

**OŚWIADCZENIE DOTYCZĄCE DEFINICJI PRZEDSIĘBIORSTWA:**

Oświadczam, że zgodnie z ROZPORZĄDZENIEM KOMISJI (UE) NR 651/2014 z dnia 17 czerwca 2014 r. jestem:

* - mikro przedsiębiorstwem
* - małym przedsiębiorstwem
* - średnim przedsiębiorstwem
* - dużym przedsiębiorstwem

\* właściwe zaznaczyć

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

…………………………………………

*(podpis)*

**Załącznik nr 1a *-*** Oświadczenie Wykonawcy o przynależności albo braku przynależności do tej samej grupy kapitałowej

*Postępowanie nr ZP/12/20*

**Nazwa i adres wykonawcy:**

**……………………………….**

…………………………….....

……………………………….

Oświadczam, że:

* nie należę do grupy kapitałowej o której mowa w art. 24 ust. 1 pkt 23 ustawy Prawo Zamówień Publicznych
* należę do grupy kapitałowej o której mowa w art. 24 ust. 1 pkt 23 ustawy Prawo Zamówień Publicznych z następującymi Wykonawcami:

1 ..................

2 ..................

3 ..................

**Informacja dla Wykonawców:**

W przypadku przynależności do tej samej grupy kapitałowej wykonawca może złożyć wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.

...................................... ......................, dnia .... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Załącznik nr 2** – Wzór umowy

**UMOWA ZP/…../20 (dla części nr 1,2,4 )**

zawarta w Krakowie, w dniu ……………….. 2019 r. pomiędzy:

Siecią Badawczą Łukasiewicz – Krakowskim Instytutem Technologicznym z siedzibą w Krakowie, 30-418 Kraków, ul. Zakopiańska 73, wpisanym do Krajowego Rejestru Sądowego przez Sąd Rejonowy dla Krakowa-Śródmieście, XI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000861401, NIP: 675-000-00-88, REGON 387116932 , reprezentowanym przez:

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

zwanym w dalszej części umowy **„Zamawiającym”**

a

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

reprezentowanym przez:

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

zwanym w dalszej części umowy **„Wykonawcą”**

po przeprowadzeniu postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz.U. z 2015 r. poz. 2164 z późn. zm.), zwanej dalej ustawą Pzp i wybraniu oferty Wykonawcy jako oferty najkorzystniejszej.

**§ 1**

**Przedmiot umowy.**

1. Na warunkach określonych niniejszą umową, Wykonawca sprzedaje Zamawiającemu ……….., zwane dalej przedmiotem zamówienia.
2. Parametry techniczne przedmiotu zamówienia, warunki licencji na oprogramowanie wchodzące w zakres przedmiotu zamówienia oraz warunki gwarancji określa załącznik nr 1 do umowy (zał. nr ……. do SIWZ) oraz oferta Wykonawcy stanowiąca załącznik nr 2 do umowy.
3. Wykonawca zobowiązuje się również do dostarczenia przedmiotu zamówienia na adres wskazany przez Zamawiającego.
4. Wykonawca zobowiązany jest do podpisania i przestrzegania Załącznika nr 3 - zobowiązania do zachowania poufności
5. Wykonawca zapewnia serwis gwarancyjny w zakresie wszelkich składowych przedmiotu umowy oraz nieodpłatne przeglądy serwisowe w okresie gwarancyjnym. Wykonawca, w ramach serwisu gwarancyjnego, zapewni także wsparcie techniczne obejmujące pomoc w weryfikacji, zgłaszaniu oraz rozwiązywaniu problemów wynikających z funkcjonowania całości przedmiotu umowy.
6. Jakakolwiek usterka lub awaria, która wystąpi w okresie gwarancji zostanie usunięta przez Wykonawcę na jego koszt i ryzyko, przy uwzględnieniu niezbędnych składowych działań zmierzających do usunięcia wady lub usterki w postaci: dojazdu serwisu na miejsce przedmiotu umowy, ewentualnego transportu sprzętu do serwisu, oraz wszelkich kosztów wymienianych części i robocizny, w tym - wszelkich, pozostałych działań zmierzających do skutecznego wypełnienia przez Wykonawcę jego zobowiązań z tytułu gwarancji. Powyższe dotyczy także każdej sytuacji zniszczenia przez którąkolwiek ze składowych przedmiotu niniejszej umowy infrastruktury Zamawiającego, w tym funkcjonujących u Zamawiającego systemów programów komputerowych i innych systemów informatycznych. W sytuacji opisanej w zdaniu uprzednim, Wykonawca przejmuje na siebie wszelkie ciężary i ryzyko naprawienia zaistniałych u Zamawiającego szkód do pełnej ich wysokości, w tym zobowiązuje się przejąć i świadczyć na rzecz Zamawiającego zobowiązania jakie wynikają z gwarancji posiadanych przez Zamawiającego na infrastrukturę, programy komputerowe oraz systemy informatyczne.
7. Zgłoszenia ewentualnych wad i usterek Zamawiający będzie dokonywał faksem lub mailem z zastrzeżeniem, że potwierdzenie prawidłowej transmisji faksu lub maila stanowi dowód skutecznego zgłoszenia przez Zamawiającego wady lub usterki. Reakcja Wykonawcy będzie polegać na: potwierdzeniu otrzymania zgłoszenia (przy pomocy faksu lub maila), przybyciu do siedziby Zamawiającego celem dokonania oględzin ewentualnej awarii lub usterki. Zamawiający dopuszcza również realizację wsparcia technicznego lub usunięcia usterki poprzez zdalny dostęp do systemu. Wsparcie techniczne realizowane będzie telefonicznie lub pocztę e-mail.
8. Stwierdzona w okresie gwarancji wada lub usterka którejkolwiek z części składowych przedmiotu umowy kwalifikuje tę część składową do naprawy lub wymiany na nową, na koszt i ryzyko Wykonawcy. Wykonawca w takim przypadku jest zobowiązany dostarczyć Zamawiającemu naprawiony (w pełni sprawny) lub nowy, wolny od wad przedmiot umowy w zakresie wszelkich jego składowych podlegających naprawie lub wymianie, o takich samych co zamówiony parametrach, w terminie do 10 dni roboczych, licząc od daty dokonania przez Zamawiającego zgłoszenia stosownego żądania faksem lub mailem (z zastrzeżeniem, iż potwierdzenie prawidłowej transmisji faksu lub maila stanowi dowód dokonania skutecznego zgłoszenia przez Zamawiającego). Czasookres naprawy którejkolwiek ze składowych przedmiotu umowy powoduje przedłużenie czasu obowiązywania udzielonej pierwotnie gwarancji w zakresie tej składowej o czas niefunkcjonowania przedmiotu umowy na skutek wad i usterek.
9. Zamawiający może wykonywać uprawnienia z tytułu gwarancji niezależnie od uprawnień z tytułu rękojmi.

**§ 2**

**Cena i warunki wykonania umowy**

* + - 1. Za wykonanie obowiązków określonych w § 1 umowy, Zamawiający zapłaci Wykonawcy kwotę ........................... brutto (słownie: ...................................... ). Kwota ta obejmuje cenę przedmiotu zamówienia wraz z kosztem transportu i wszelkimi obowiązkami wynikającymi z zawartej umowy, w tym kosztami licencji potrzebnych do korzystania z oprogramowania wchodzącego w zakres przedmiotu zamówienia.
      2. Umowa zostanie zrealizowana najpóźniej w terminie ……………………..
      3. O terminie dostawy przedmiotu zamówienia Wykonawca zawiadomi Zamawiającego z trzydniowym wyprzedzeniem. Wykonawca dostarczy Zamawiającemu przedmiot zamówienia na własny koszt i ryzyko. W szczególności, Wykonawca ponosi odpowiedzialność za utratę, zniszczenie lub uszkodzenie przedmiotu zamówienia w trakcie transportu lub montażu.
      4. Wykonawca udziela gwarancji na zasadach określonych w załączniku nr 1 do umowy(zał. nr …….….. do SIWZ)

**§ 3**

**Odbiór i warunki płatności**.

* + - 1. Odbiór odbędzie się po dostarczeniu przedmiotu zamówienia, w wyniku którego zostanie sporządzony przez przedstawicieli obu stron protokół, sporządzony w formie pisemnej i podpisany przez obie strony.
      2. Zapłata należności nastąpi przelewem wterminie 30 dni od daty otrzymania faktury, wystawionej w oparciu o protokół odbioru, o którym mowa w ust.1, z którego wynika, że Zamawiający nie zgłasza zastrzeżeń.
      3. Brak uwag do protokołu, nie uchybia prawu Zamawiającego do wysuwania roszczeń z tytułu nienależytego wykonania umowy, a w szczególności z tytułu rękojmi, w przypadku późniejszego wykrycia lub ujawnienia wad.

**§ 4**

**Odpowiedzialność odszkodowawcza.**

* + - 1. W razie nieterminowego wykonania umowy Zamawiający może naliczyć karę umowną z tego tytułu w wysokości 0.2% kwoty określonej w § 2 ust. 1 za każdy dzień zwłoki, licząc od następnego dnia po terminie wskazanym w § 2 ust. 2.
      2. Jeśli zwłoka w wykonaniu umowy przekracza 30 dni, Zamawiający może od umowy odstąpić, naliczając z tego tytułu karę umowną w wysokości 20 % kwoty określonej w § 2 ust. 1, niezależnie od kary umownej naliczonej na podstawie ust. 1.
      3. W razie nieterminowego wykonywania obowiązków wynikających z rękojmi lub z udzielonej gwarancji, Zamawiający może naliczyć karę umowną z tego tytułu w wysokości 0.2% ceny określonej w § 2 ust. 1 za każdy dzień zwłoki, licząc od następnego dnia po wyznaczonym terminie.
      4. Strony dopuszczają możliwość dochodzenia odszkodowania uzupełniającego na zasadach ogólnych ponad zastrzeżone kary umowne.

**§ 5**

**Postanowienia dodatkowe**

Ewentualne koszty związane z zawarciem i realizacją umowy niewymienione w umowie obciążają Wykonawcę.

Wykonawca nie może dokonać cesji wierzytelności wynikających z niniejszej umowy bez zgody Zamawiającego wyrażonej w formie pisemnej, pod rygorem nieważności.

**§ 6**

**Postanowienia końcowe.**

* + - 1. W sprawach nieuregulowanych niniejszą umową zastosowanie mieć będą przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności. Zmiany umowy są dopuszczalne bez ograniczeń w zakresie dozwolonym przez art. 144 ustawy Prawo Zamówień Publicznych.
      2. Wszelkie spory wynikające z niniejszej umowy lub związane z jej wykonaniem rozstrzygać będzie sąd powszechny właściwy ze względu na siedzibę Zamawiającego.
      3. Załączniki stanowią integralną część umowy:

a. załącznik nr 1- OPZ- Parametry techniczne przedmiotu umowy, gwarancja,

b. załącznik nr 2 - Oferta Wykonawcy

c. załącznik nr 3 - zobowiązanie do zachowania poufności

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

***Wykonawca* *Zamawiający***

**…………………. ……………………**

**UMOWA ZP/…../20 (dla części nr 3,5,6,7 )**

zawarta w Krakowie, w dniu ……………….. 2019 r. pomiędzy:

Siecią Badawczą Łukasiewicz – Krakowskim Instytutem Technologicznym z siedzibą w Krakowie, 30-418 Kraków, ul. Zakopiańska 73, wpisanym do Krajowego Rejestru Sądowego przez Sąd Rejonowy dla Krakowa-Śródmieście, XI Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000861401, NIP: 675-000-00-88, REGON 387116932 , reprezentowanym przez:

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

zwanym w dalszej części umowy **„Zamawiającym”**

a

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

reprezentowanym przez:

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

zwanym w dalszej części umowy **„Wykonawcą”**

po przeprowadzeniu postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz.U. z 2015 r. poz. 2164 z późn. zm.), zwanej dalej ustawą Pzp i wybraniu oferty Wykonawcy jako oferty najkorzystniejszej.

**§ 1**

**Przedmiot umowy.**

1. Na warunkach określonych niniejszą umową, Wykonawca sprzedaje Zamawiającemu ……….., zwane dalej przedmiotem zamówienia.
2. Parametry techniczne przedmiotu zamówienia, warunki licencji na oprogramowanie wchodzące w zakres przedmiotu zamówienia określa załącznik nr 1 do umowy (zał. nr ……. do SIWZ) oraz oferta Wykonawcy stanowiąca załącznik nr 2 do umowy.
3. Wykonawca zobowiązuje się również do dostarczenia przedmiotu zamówienia na adres wskazany przez Zamawiającego.
4. Wykonawca zobowiązany jest do podpisania i przestrzegania Załącznika nr 3 - zobowiązania do zachowania poufności

**§ 2**

**Cena i warunki wykonania umowy**

1. Za wykonanie obowiązków określonych w § 1 umowy, Zamawiający zapłaci Wykonawcy kwotę ........................... brutto (słownie: ...................................... ). Kwota ta obejmuje cenę przedmiotu zamówienia wraz z kosztem transportu i wszelkimi obowiązkami wynikającymi z zawartej umowy, w tym kosztami licencji potrzebnych do korzystania z oprogramowania wchodzącego w zakres przedmiotu zamówienia.
2. Umowa zostanie zrealizowana najpóźniej w terminie ……………………..

**§ 3**

**Odbiór i warunki płatności**.

1. Odbiór odbędzie się po dostarczeniu przedmiotu zamówienia, w wyniku którego zostanie sporządzony przez przedstawicieli obu stron protokół, sporządzony w formie pisemnej i podpisany przez obie strony.
2. Zapłata należności nastąpi przelewem wterminie 30 dni od daty otrzymania faktury, wystawionej w oparciu o protokół odbioru, o którym mowa w ust.1, z którego wynika, że Zamawiający nie zgłasza zastrzeżeń.
3. Brak uwag do protokołu, nie uchybia prawu Zamawiającego do wysuwania roszczeń z tytułu nienależytego wykonania umowy, a w szczególności z tytułu rękojmi, w przypadku późniejszego wykrycia lub ujawnienia wad.

**§ 4**

**Odpowiedzialność odszkodowawcza.**

1. W razie nieterminowego wykonania umowy Zamawiający może naliczyć karę umowną z tego tytułu w wysokości 1% kwoty określonej w § 2 ust. 1 za każdy dzień zwłoki, licząc od następnego dnia po terminie wskazanym w § 2 ust. 2.
2. Jeśli zwłoka w wykonaniu umowy przekracza 30 dni, Zamawiający może od umowy odstąpić, naliczając z tego tytułu karę umowną w wysokości 20 % kwoty określonej w § 2 ust. 1, niezależnie od kary umownej naliczonej na podstawie ust. 1.
3. Strony dopuszczają możliwość dochodzenia odszkodowania uzupełniającego na zasadach ogólnych ponad zastrzeżone kary umowne.

**§ 5**

**Postanowienia dodatkowe**

1. Ewentualne koszty związane z zawarciem i realizacją umowy niewymienione w umowie obciążają Wykonawcę.
2. Wykonawca nie może dokonać cesji wierzytelności wynikających z niniejszej umowy bez zgody Zamawiającego wyrażonej w formie pisemnej, pod rygorem nieważności.

**§ 6**

**Postanowienia końcowe.**

1. W sprawach nieuregulowanych niniejszą umową zastosowanie mieć będą przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności. Zmiany umowy są dopuszczalne bez ograniczeń w zakresie dozwolonym przez art. 144 ustawy Prawo Zamówień Publicznych.
2. Wszelkie spory wynikające z niniejszej umowy lub związane z jej wykonaniem rozstrzygać będzie sąd powszechny właściwy ze względu na siedzibę Zamawiającego.
3. Załączniki stanowią integralną część umowy:

a. załącznik nr 1- OPZ- Parametry techniczne przedmiotu umowy

b. załącznik nr 2 - Oferta Wykonawcy

c. załącznik nr 3 - zobowiązanie do zachowania poufności

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

***Wykonawca* *Zamawiający***

**…………………. ……………………**

Załącznik

**ZOBOWIĄZANIE DO ZACHOWANIA POUFNOŚCI**

Ja, <*imię, nazwisko*>, zwany dalej Przyjmującym zobowiązanie, wykonując zadania w imieniu <*nazwa podmiotu – strony umowy*>, polegające na <*zakres działań i odwołanie do umowy*> zobowiązuję się do zachowania w tajemnicy i ochrony informacji poufnych, Administratorem których jest Sieć Badawcza Łukasiewicz – Krakowski Instytut Technologiczny w Krakowie, zwany dalej: Instytut, które pozyskałem w związku z zadaniami wynikającymi z podjętej współpracy/umowy.

Przyjmuję do wiadomości, że:

1. Informacją poufną jest każda informacja za wyjątkiem informacji wyraźnie oznaczonej jako ogólnie dostępna, informacji udostępnionej publicznie lub informacji klasyfikowanej jako informacja publiczna.

Szczególnie informacjami poufnymi są: dane medyczne, dane osobowe, informacje o środkach, środowisku i metodach pracy Instytutu, w tym informacje o procesach, politykach, procedurach i instrukcjach. Sposób przetwarzania ww. informacji nie wpływa na klasyfikację informacji jako poufnych.

2. Zobowiązanie do zachowania w tajemnicy i ochrony informacji poufnych rozumiane jest jako:

a. Nie ujawnianie stronom trzecim informacji poufnych oraz zachowanie staranności w działaniu w celu utrzymania ww. informacji w tajemnicy.

b. Nie kopiowanie i niepowielanie informacji poufnych w celach innych niż realizacja zadań będących przedmiotem współpracy/umowy.

c. Spełnienie ustawowych wymagań związanych z dostępem do danych (jeżeli zakres świadczonej usługi wiąże się z dostępem do danych osobowych: uczestnictwo w szkoleniu z tego zakresu oraz uzyskanie upoważnienia dostępu do tych danych przed realizacją usługi na rzecz Instytutu)[[1]](#footnote-1).

d. Zwrot Instytutowi informacji poufnych łącznie z kopiami oraz usunięcie tych informacji z wszystkich systemów przetwarzania i przechowywania danych Przyjmującego zobowiązanie – za wyjątkiem sytuacji, w których przechowywanie kopii danych poufnych przez Przyjmującego zobowiązanie wynika z umowy i/lub odrębnych przepisów prawa.

3. Zobowiązanie do zachowania poufności jest wyłączone w stosunku do informacji poufnych, które muszą zostać ujawnione z tytułu orzeczenia sądu lub decyzji administracyjnej wydanej na podstawie obowiązujących przepisów prawa, pod warunkiem, że Przyjmujący zobowiązanie jest stroną

w postępowaniu przed sądem lub stroną decyzji administracyjnej zobowiązującej do wyjawienia informacji otrzymanych na podstawie niniejszego zobowiązania.

4. Zobowiązanie do zachowania poufności jest wyłączone w stosunku do osób, które wskaże na piśmie Instytut.

5. Dane osobowe Przyjmującego zobowiązanie są przetwarzane przez Instytut z tytułu realizacji umowy między stronami, której stroną jest ww. Dane osobowe Przyjmującego zobowiązanie nie będą udostępniane, a Przyjmujący zobowiązanie ma prawo do wglądu do tych danych i żądania korekty, w sytuacji, kiedy dane będą niezgodne ze stanem faktycznym. Zakres przetwarzanych danych jest ograniczony do danych wymienionych w umowie oraz danych potwierdzających możliwość jej realizacji przez Przyjmujący zobowiązanie.

………………………………………………………………………

Data i Podpis przyjmującego zobowiązanie

(Zobowiązanie obowiązuje od daty jego złożenia

**Opis przedmiotu zamówienia – zał nr 3.**

**CZĘŚĆ I**

**Cluster systemów bezpieczeństwa – 2 komplety**

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall musi dysponować minimum:

* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System musi być wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

**Polityki, Firewall**

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure
* Cisco ACI.
* Google Cloud Platform (GCP).
* Nuage Networks VSP.
* OpenStack.
* VMware vCenter (ESXi).
* VMware NSX.

**Połączenia VPN**

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

* Wsparcie dla IKE v1 oraz v2.
* Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19 i 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

**Routing i obsługa łączy WAN**

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

* Routingu statycznego.
* Policy Based Routingu.
* Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

**Zarządzanie pasmem**

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

**Ochrona przed atakami**

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

**Kontrola WWW**

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

**Logowanie**

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

**Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

**Serwisy i licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

**Gwarancja oraz wsparcie**

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Opisy do wymagań ogólnych**

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

**CZĘŚĆ II**

**Zakup i dostawa macierzy flash – 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa parametru** | **Minimalna wartość parametru** |
|  | Obudowa | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | Pojemność: | System musi zostać dostarczony w konfiguracji zawierającej minimum  9 dysków 1600GB SSD  i zajmować maksymalnie 2U w szafie rack  System musi ponadto wspierać dyski:  - SSD: od 800GB do 15.3TB  - SAS 10k od 900GB do 1800GB  - NL-SAS od 4TB do 12TB  System musi mieć możliwość rozbudowy do minimum 120 dysków oraz musi pozwalać na rozbudowę do wyższych modeli bez potrzeby migracji danych (przez rozbudowę do wyższego modelu zamawiający rozumie do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami). Zamawiający dopuszcza rozwiązanie, które nie pozwala na taką rozbudowę w przypadku, gdy zostanie zaoferowany najwyższy z modeli macierzy skalowalny min do 500 dysków oraz pamięcią cache min 512GB. |
|  | Kontroler | Dwa kontrolery wyposażone w przynajmniej 8GB cache każdy.  W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash.  System musi pozwalać na rozbudowę do 32GB pamięci cache na kontroler |
|  | Interfejsy | Oferowana macierz musi posiadać minimum  - 4 porty FC 10GbE SFP+ do podłączenia hostów  - 4 porty SAS 12 Gb/s do podłączenia półek dyskowych  oraz pozwalać na rozbudowę o dodatkowe 8 portów 10GbE SFP+ do podłączenia hostów. |
|  | RAID | Wsparcie dla RAID: 0, 1, 5, 6, 10  Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych.  Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane wsposób sprzętowy przez dedykowany układ w macierzy. |
|  | Obsługiwane protokoły | FC, iSCSI , SAS oraz S3  Technologia macierzy w przypadku rozbudowy o porty FC musi pozwalać na zmianę udostępniania danych z FC na iSCSI i na odwrót bez zmiany wkładek SFP+. Zamawiający pozwala na dostarczenie macierzy, która nie spełnia tego warunku przy założeniu zaoferowania rozwiązania od razu wyposażonego w:  12 portów FC 16Gb  12 portów 10GbE SFP+  Realizację protokołu S3 zamawiający dopuszcza za pomocą software define Storage. |
|  | Inne wymagania | Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów:  Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®, Oracle® Solaris, HP HP-UX, IBM AIX,  Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen.  Macierz musi posiadać funkcjonalność klonowania danych  Macierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) w trybie synchronicznym i asynchronicznym, system musi pozwalać na wykonanie do 32 jednoczesnych replikacji.  Macierz musi pozwalać na replikację natywną z istniejącą macierzą E2800 z zachowaniem wsparcia przez producenta macierzy netapp na taką replikację,  Macierz musi posiadać możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. ThinProvisioning).  Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.  Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji.  Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika.  Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID.  Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD.  Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków  Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:  - wydajności i opóźnień na wolumenach  - wydajności I/Ops, MB/s  Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.  Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z:  - Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter  - VMware VASA  - Vmware SRM  - MicrosoftVirtual Disk Service (VDS)  - Microsoft Virtual Shadow Service (VSS)  - Oracle Enterprise Manager – monitoring zasobów macierzowych  Zamawiający dopuszcza zaoferowania zewnętrznego oprogramowania do zapewnienia integracji i monitoring w/w aplikacji np. w formie Software Definestorage.  Macierz musi pozwalać na szyfrowania danych, realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.  Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. |
|  | Gwarancja i serwis | 3 lata serwisu producenta zapewniającego dostawę podzespołu zapasowego na następny dzień roboczy od diagnozy problemu. Możliwość zgłaszania awarii poprzez linię telefoniczną lub inne systemy firmy serwisującej.  Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. |

**CZĘŚĆ III**

1. Przedmiotem zamówienia jest przedłużenie usługi wsparcia technicznego producenta na kolejny rok dla infrastruktury macierzy dyskowych posiadanych przez Zamawiającego. Przedmiot zamówienia obejmuje wsparcie dla następujących urządzeń:
   1. Macierz HPE MSA 1040 2Prt 1G iSCSI DC LFF Strg o numerze seryjnym: 2S6526C024
   2. Macierz HPE MSA 1040 2Prt FC DC SFF Strg o numerze seryjnym: 2S6513B400.
2. Obecnie posiadana usługa wsparcia technicznego (HPE Foundation Care NBD SVC) urządzeń obowiązuje do:
   1. HPE MSA 1040 2Prt 1G iSCSI DC LFF Strg do dnia 6 października 2020
   2. HPE MSA 1040 2Prt FC DC SFF Strg do dnia 7 października 2020.
3. Zakres wsparcia technicznego
   1. Oferowana usługa wsparcia dla urządzeń wymienionych w pkt 2) ma być świadczona w trybie NBD (next business day - następny dzień roboczy).
   2. Wykonawca dostarczy dokumenty potwierdzające gwarancję producenta dla sprzętu, o którym mowa w punkcie 2) zarejestrowane na Zamawiającego, obejmujące datę uruchomienia kontraktu serwisowego, model, numery seryjne oraz zapisy warunków gwarancji producenta.
   3. Wsparcie musi być aktywowane do 7 dni, liczonych od daty udzielenia zamówienia, tj. zawarcia umowy na okres wskazany w ppkt. 3.a.
   4. Oferowana usługa wsparcia musi zapewniać ciągłość kontraktów serwisowych wygasających w terminach wymienionych w pkt.2).

**CZĘŚĆ IV**

**Dysk zewnętrzny – 1 szt.**

|  |  |
| --- | --- |
| **Nazwa parametru** | **Wymagane minimalne parametry techniczne** |
| Typ | Dysk zewnętrzny SSD |
| Zastosowanie | Dysk wykorzystywany do przenoszenia danych związanych z prowadzonymi badaniami |
| Rodzaj | SSD |
| Format | 2,5” |
| Pojemność | 1TB |
| Interfejs | USB 3.1 (Gen 2) |
| Prędkość odczytu | 550 MB/s |
| Klasa wytrzymałości | IP55 |
| Kompatybilność | Windows 10, Windows 8, Windows 7, Windows Vista, Mac OS 10.4+ |
| Dodatkowe informacje | Odporność na zachlapanie  Kurzoodporność  Zwiększona odporność na drgania |
| Dodatkowe wyposażenie | Dedykowany kabel USB |
| Gwarancja | 36 miesięcy |

**CZĘŚĆ V**

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Skrócona nazwa | Typ licencji | Liczba licencji w sztukach |
| 1 | Windows Server User CAL | Per User | 100 |
| 2 | Windows Server Standard Core 2 SL | Core License | 2 |

1. Wykonawca dostarczy wyżej wymienione lub równoważne licencje i oprogramowanie w formie elektronicznej lub umożliwi ich pobranie ze strony producenta wraz z kluczami niezbędnym do ich poprawnej instalacji i użytkowania.
2. Dostarczone licencje powinny być zgodne z dostarczaną wersją oprogramowania.
3. Wykonawca dostarczy bezterminowych licencji na oprogramowanie. Zamawiający oświadcza, że jest jednostką naukową, funkcjonującą jako instytut badawczy na podstawie ustawy o instytutach badawczych. Prowadzi badania naukowe i prace rozwojowe. Nie działa dla zysku. Nie prowadzi działalności edukacyjnej w zakresie szkolnictwa wyższego ani zawodowego.
4. Wykonawca zobowiązuje się dostarczyć wyżej wymienione oprogramowanie w najnowszych dostępnych wersjach.

**CZĘŚĆ VI**

|  |  |
| --- | --- |
| **Nazwa parametru oprogramowania** | **Wymagane minimalne parametry techniczne oprogramowania** |
| Typ oprogramowania | Oprogramowanie służące do obróbki grafiki komputerowej w tym grafiki wektorowej |
| Rodzaj licencji | Edukacyjna, wieczysta (dożywotnia) |
| Ilość stanowisk | 1 |
| Wersja językowa | polska |
| Wersja językowa interfejsu użytkownika | polska |
| Obsługiwane formaty plików (odczyt oraz zapis) | Adobe Illustrator (AI)  Czcionka Adobe Type 1 (PFB)  Mapa bitowa Windows (BMP)  Mapa bitowa systemu OS/2 (BMP)  Computer Graphics Metafile (CGM)  CorelDRAW (CDR)  Corel Presentation Exchange (CMX)  Corel PHOTO-PAINT (CPT)  Biblioteka symboli firmy Corel (CSL)  Zasób wskaźników myszy (CUR)  Pliki Microsoft Word (DOC, DOCX lub RTF)  Microsoft Publisher (PUB)  Corel DESIGNER (DES, DSF, DS4 lub DRW)  AutoCAD Drawing Database (DWG) i AutoCAD Drawing Interchange Format (DXF)  Encapsulated PostScript (EPS)  PostScript (PS lub PRN)  GIF  JPEG (JPG)  JPEG 2000 (JP2)  Obrazek Kodak Photo CD (PCD)  PICT (PCT)  PaintBrush (PCX)  Adobe Portable Document Format (PDF)  Plik plotera HPGL (PLT)  Portable Network Graphics (PNG)  Adobe Photoshop (PSD)  Corel Painter (RIF)  Scalable Vector Graphics (SVG)  Adobe Flash (SWF)  TARGA (TGA)  TIFF  Corel Paint Shop Pro (PSP)  TrueType Font (TTF)  Pliki Visio (VSD)  WordPerfect Document (WPD)  WordPerfect Graphic (WPG)  Formaty plików RAW z aparatu fotograficznego  Mapa bitowa z kompresją falkową (WI)  Windows Metafile Format (WMF) |
| Funkcje | Tworzenie i edycja grafiki wektorowej oraz rastrowej;  Narzędzia do projektowania stron internetowych;  Rozszerzalność programu za pomocą ‘wtyczek’;  Tryb symetrii;  Dodawanie blokowych cieni wektorowych do obiektów i tekstu;  Tworzenie mozaik wektorowych z dowolnej liczby wybranych obiektów wektorowych lub map bitowych;  Narzędzie cień wewnętrzny;  Wtapianie wektorowe;  Soczewki efektów map bitowych;  Narzędzie Uderzenie - dodawanie ruchu lub wyróżnienia do elementu na rysunku;  Funkcja wyrównania i rozmieszczenia węzłów;  Prostowanie zdjęć - wyprostowanie przekrzywionych obrazów przez wyrównanie paska prostującego z elementem obrazka;  Niestandardowe kształty węzłów;  Wypełnienie deseniami wektorowymi oraz z mapy bitowej;  Wypełnienie tonalne;  Ukrywanie i wyświetlanie obiektów oraz grup obiektów;  Tworzenie i zapisywanie wypełnień mapą bitową lub deseniem wektorowym na podstawie obiektów zaznaczonych na obszarze roboczym;  Wypełnienie siatkowe;  Wygładzanie obiektów wektorowych - usuwanie postrzępionych krawędzi i zmniejszanie liczby węzłów w obiektach złożonych z krzywych;  Opcje nadpróbkowania;  Usuwanie artefaktów JPEG;  Narzędzie Inteligentna maska wyboru - zaznaczenie obszarów obrazka z wykorzystaniem algorytmu, który inteligentnie rozszerza zaznaczenie, szukając krawędzi;  Tworzenie kolaży ze zdjęć;  Scalanie zdjęć HDR;  Narzędzie klonowanie korygujące - usuwanie niedoskonałości, zamalowując je teksturą dobraną do obszaru otoczenia;  Soczewka Maska wyostrzająca - wyostrzanie zdjęcia poprzez zwiększenie kontrastu sąsiednich pikseli przy zachowaniu szczegółów takich elementów jak krawędzie i duże struktury;  Narzędzie Maska planarna - zdefiniowanie wtapianego obszaru do edycji przy zastosowaniu linii równoległych;  Inteligentne skalowanie - usuwanie niechcianych fragmentów z fotografii z jednoczesnym dostosowaniem proporcji zdjęcia;  Tryb scalania z przekazywaniem;  Dopasowywanie krzywej totalnej - dostosowanie tonu obrazu;  Obsługa czcionek zmiennych;  Obsługa wielopoziomowych list punktowanych i numerowanych;  Stosowanie wypełnień i przezroczystości oraz zarządzanie nimi;  Importowanie obszarów roboczych z poprzednich wersji CorelDrRAW;  Obsługa obszarów roboczych;  Zaawanasowana obsługa wielu monitorów;  Wzorce pustych dokumentów/obrazów;  Włączanie i wyłączanie przyciągania;  Dopasowywanie obiektów do ścieżki - umieszczanie dowolnej liczby dowolnego rodzaju obiektów na wybranej ścieżce;  Stosowanie obwiedni do map bitowych - kształtowanie map bitowych, przyciągając węzły ograniczające kształtowany obszar;  Dodawanie numerów stron;  Interakcyjne ramki - wypełnianie obiektów szybkiego kadrowania grafiką zastępczą i ramkami tekstowymi;  Tworzenie i importowanie tabel z możliwością stosowania strukturalnego układu tekstu i grafiki;  Tworzenie kodów QR oraz kodów paskowych;  Prowadnice wyrównania i dynamiczne - wyświetlanie, ustawianie i modyfikowanie prowadnic wyrównania;  Wbudowana obsługa plików RAW z aparatów fotograficznych - importowanie i dostosowanie plików RAW bezpośrednio z aparatu cyfrowego;  Opcja wydruku seryjnego;  Obsługa procesorów wielordzeniowych;  Korekcja zniekształceń obiektywu;  Filtr czcionek według uprawnień do osadzania;  Efekt dodaj perspektywę m.in. do map bitowych;  Tworzenie prostych animacji flash;  Podział obrazu na warstwy;  Modyfikacja pędzli; |
| Zgodność z formatami plików utworzonych w programach graficznych | CorelDraw Graphics Suite X6  CorelDraw Graphics Suite X7  CorelDraw Graphics Suite X8 |
| Sposób dostawy | Dystrybucja cyfrowa |
| Obsługiwane systemy operacyjne | Microsoft Windows 7 wersja polska  Microsoft Windows 8.1 wersja polska  Microsoft Windows 10 wersja polska |
| Inne | Dostępna pełna dokumentacja w języku polskim |

Za oprogramowanie równoważne opisanemu w specyfikacji przy pomocy nazwy uznaje się oprogramowanie posiadające następujące cechy:

1. Warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja na oprogramowanie wskazane przez Zamawiającego.
2. Zakres funkcjonalny oprogramowania jest w pełni zgodny z zakresem funkcjonalnym oprogramowania wskazanego przez Zamawiającego.
3. Formaty danych wejściowych i wyjściowych są identyczne i odpowiadają przynajmniej liczbie i typowi formatów dla oprogramowania wskazanego przez Zamawiającego.

Wraz z produktem równoważnym Wykonawca jest zobowiązany do dostarczenia następujących dokumentów:

* pełnego postanowienia licencji/sublicencji produktu równoważnego,
* pełnego wykazu funkcjonalności produktu równoważnego,
* pełnych warunków i zasad świadczenia usług gwarancji, serwisu pogwarancyjnego, asysty technicznej i konserwacji dla produktu równoważnego.

W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego.

Dodatkowe wymagania dla produktu równoważnego:

1. Nabycie licencji oprogramowania równoważnego pozwala na legalne używanie posiadanych przez Zamawiającego licencji oprogramowania.
2. Oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego.
3. Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego.
4. Oprogramowanie równoważne nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowaniem.
5. W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego.

**CZĘŚĆ VII**

Zwiększenie o 150 stanowisk licencji ważnej do 11 lutego 2022 r. na posiadane przez Zamawiającego oprogramowanie antywirusowe ESET Endpoint Antivirus Suite

Zaoferowane dodatkowe licencje muszą współpracować z wykorzystywanym przez Zamawiającego centralnym serwerem zarządzającym oprogramowaniem ESET Endpoint Antivirus Suite.

Zamawiający posiada licencję ESET Endpoint Antivirus Suite na 200 stanowisk ważną do 11 lutego 2022r.

Zamawiający dopuszcza możliwość dostarczenia produktu równoważnego o właściwościach, funkcjonalnościach i parametrach nie gorszych od wskazanych niżej. W przypadku dostarczenia oprogramowania równoważnego rekonfiguracja stacji roboczych, serwera plików, systemów wirtualizacji oraz inne prace niezbędne do prawidłowego funkcjonowania przedmiotu zamówienia u Zamawiającego leżą po stronie Wykonawcy i odbędą się na jego koszt.

Oprogramowanie równoważne:

**Wymagania ogólne:**

1. Wykonawca zobowiązany jest do dostarczenia licencji na oferowany system antywirusowy – 350 licencji na ochronę:
   1. stacji roboczych
   2. urządzeń mobilnych
   3. serwerów plikowych (przy czym liczba chronionych serwerów nie będzie większa niż 30% ogólnej liczby zakupionych licencji)

ważnych do 11 lutego 2022r.

1. Wykonawca dostarczy konsolę centralnej administracji oprogramowania antywirusowego za pomocą, której możliwa będzie zdalna instalacja oprogramowania na stacjach roboczych i serwerach oraz pełny podgląd stanu ochrony sieci dla wszystkich 350 licencji.
2. Wykonawca udzieli bezpłatnego dostępu do opartego na chmurze systemu licencjonowania który pozwoli na kontrolę, raportowanie i przegląd posiadanych licencji.
3. Wykonawca zobowiązuje się udzielić wsparcia technicznego (na taki sam okres, na który zostanie udzielona licencja) opartego o świadczenie gwarancyjne producenta oprogramowania.
4. Polskojęzyczny interfejs oprogramowania antywirusowego instalowanego na stacjach roboczych i serwerach oraz konsoli do centralnego zarządzania oprogramowaniem antywirusowym.
5. Możliwość aktualizacji oprogramowania antywirusowego oraz konsoli do centralnego zarządzania oprogramowaniem antywirusowym do najnowszej wersji udostępnionej przez producenta.
6. Oprogramowanie antywirusowe musi posiadać certyfikaty niezależnych laboratoriów.
7. Program musi wspierać następujące platformy:
8. Microsoft Windows 10 Professional x86 Edition
9. Microsoft Windows 10 Professional x64 Edition
10. Microsoft Windows 8.1 Enterprise x86 Edition
11. Microsoft Windows 8.1 Enterprise x64 Edition
12. Microsoft Windows 8 Professional / Enterprise x86 Edition
13. Microsoft Windows 8 Professional / Enterprise x64 Edition
14. Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition
15. Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition
16. Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP
17. Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
18. Microsoft Windows Vista x86 Edition SP2
19. Microsoft Windows Vista x64 Edition SP2
20. Microsoft Windows Server 2016 Standard
21. Microsoft Windows Server 2012 R2 Standard x64
22. Microsoft Windows Server 2012 Standard x64
23. Microsoft Windows Server 2008 R2 Standard / Enterprise (x64 SP0 lub nowszy)
24. Microsoft Windows Server 2008 Standard / Enterprise SP2

**Wymagania techniczne dla ochrony stacji roboczych:**

1. Program musi posiadać wbudowaną ochronę dostępu do danych oraz zabezpieczenie przed wszystkimi rodzajami zagrożeń, m.in. przed wirusami, rootkitami, robakami oraz przed oprogramowaniem szpiegującym.
2. Program musi chronić przed stronami internetowymi, które podszywają się pod zaufane serwisy WWW i próbują zdobyć poufne informacje.
3. Program musi kontrolować urządzenia i blokować nieautoryzowane nośniki danych. Program daje możliwość tworzenia reguł w oparciu o grupy użytkowników w celu dopasowania do polityki bezpieczeństwa.
4. Program musi posiadać możliwość zdefiniowania reguł dla rejestru systemu, procesów, aplikacji i plików. Program musi wykryć infekcje mające na celu zmniejszenie wydajności systemu operacyjnego.
5. Program musi zapobiegać włamaniom, monitorować aktywność wszystkich procesów systemu i wykorzystywać predefiniowane reguły do rozpoznawania podejrzanego działania systemu. W razie wykrycia takiej aktywności system automatycznie unieszkodliwi działanie złośliwego procesu.
6. Program musi zapewnić ochronę przed niebezpiecznymi rodzajami aktywności sieciowej i atakami. Dać możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
7. System musi blokować programy typu exploit. Blokować zagrożenia i ataki, które unikają wykrycia przez tradycyjne oprogramowanie antywirusowe.
8. Program musi eliminować zagrożenia blokujące komputer i wyłudzające okup, chronić przed atakami, wykorzystującymi luki w przeglądarkach internetowych, czytnikach PDF, komponentach pakietu Office, klientach pocztowych czy oprogramowaniu Java.
9. Program musi leczyć i usuwać pliki z archiwów następujących formatów: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
10. Program musi posiadać zaawansowany skaner pamięci który zabezpieczy przed skomplikowanymi zagrożeniami, wielokrotnie spakowanymi lub zaszyfrowanymi.
11. Program musi chronić przed złośliwym oprogramowaniem dedykowanym na inne systemy operacyjne.
12. Program musi pozwalać na automatyczne skanowanie zaraz po instalacji na stacji roboczej.
13. Monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego.
14. Program musi pozwolić na przywrócenie poprzedniej wersji modułów ochrony i bazy sygnatur wirusów oraz w razie potrzeby umożliwia wstrzymanie aktualizacji na określony czas lub do momentu ręcznego uruchomienia.
15. Program podczas instalacji musi wykryć, usunąć i zastąpić inne oprogramowanie zabezpieczające (wersje 32-bitowe oraz wersje 64-bitowe) zainstalowane na komputerze.
16. Program musi umożliwiać administratorowi dostosowywanie trybu GUI programu na stacji roboczej użytkownika.
17. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nieposiadających uprawnień administracyjnych.
18. Program musi pozwalać na aktualizację baz sygnatur wirusów z poziomu programu zainstalowanego na stacji roboczej użytkownika.
19. Program ma możliwość skanowania i klasyfikowania plików na podstawie informacji gromadzonych w oparciu o technologie chmury.
20. Program musi klasyfikować wszystkie aplikacje i ograniczać ich działania na podstawie ich stanu.
21. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
22. Możliwość określenia poziomu czułości modułu heurystycznego.
23. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.
24. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
25. Możliwość wysyłania podejrzanego obiektu do producenta oprogramowania antywirusowego w celu analizy.
26. Program posiada możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
27. Program musi posiadać możliwość zablokowania hasłem operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu.
28. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju.
29. Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
30. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.

**Wymagania techniczne dla ochrony serwerów:**

1. Program musi posiadać wbudowaną ochronę dostępu do danych oraz zabezpieczenie przed wszystkimi rodzajami zagrożeń, m.in. przed wirusami, rootkitami, robakami oraz oprogramowaniem szpiegującym.
2. Program ma możliwość skanowania i klasyfikowania plików na podstawie informacji gromadzonych w oparciu o technologie chmury.
3. Program musi mieć możliwość klasyfikacji wszystkich aplikacji i możliwość ograniczenia ich działania na podstawie ich stanu.
4. Wbudowany moduł wyszukiwania heurystycznego bazującego na analizie kodu potencjalnego wirusa.
5. Możliwość określenia poziomu czułości modułu heurystycznego.
6. Terminarz pozwalający na planowanie zadań, w tym także terminów automatycznej aktualizacji baz sygnatur.
7. Program posiada możliwość zresetowania wszystkich ustawień włącznie z regułami stworzonymi przez użytkownika.
8. Program musi posiadać możliwość zablokowania hasłem operacji zamykania programu, zatrzymywania zadań, wyłączania ochrony, wyłączania profilu administracyjnego, zmiany ustawień, usunięcia licencji oraz odinstalowania programu.
9. Program musi posiadać możliwość cofnięcia ostatniej aktualizacji w przypadku uszkodzenia zestawu uaktualnień.
10. Możliwość zablokowania dostępu do ustawień programu dla użytkowników nieposiadających uprawnień administracyjnych.
11. Program musi posiadać możliwość określenia ustawień serwera proxy w przypadku, gdy jest on wymagany do nawiązania połączenia z Internetem.
12. Leczenie i usuwanie plików z archiwów następujących formatów: RAR, ARJ, ZIP, CAB, LHA, JAR i ICE.
13. Biała lista bezpiecznych plików bazująca na reputacji obiektów w chmurze dla szybszego skanowania. Tylko informacje o plikach wykonywalnych i archiwach wysyłane są do chmury – wysyłane dane są w pełni anonimowe.
14. Program przechowuje dane dotyczące skanowanych plików, dzięki czemu nie są one ponownie sprawdzane na innych maszynach wirtualnych. Aktualizacje baz sygnatur wirusów i modułów aplikacji przechowywane są poza domyślną lokalizacją, nie ma konieczności ich ponownego pobierania w przypadku przywrócenia migawki maszyny wirtualnej.
15. Program musi eliminować zagrożenia blokujące komputer i wyłudzające okup. Chroni przed atakami, wykorzystującymi luki w przeglądarkach internetowych, czytnikach PDF, komponentach pakietu Office, klientach pocztowych czy oprogramowaniu Java.
16. Program musi posiadać zaawansowany skaner pamięci który zabezpieczy przed skomplikowanymi zagrożeniami, wielokrotnie spakowanymi lub zaszyfrowanymi.
17. Umożliwia skonfigurowanie rozwiązania tak, aby automatycznie replikowało swoje ustawienia po zainstalowaniu w środowisku klastrowym. Kreator umożliwi przeniesienie konfiguracji pomiędzy wieloma instancjami programu oraz zarządzanie nimi jako całością.
18. Program pozwoli na konfigurację skanowania na żądanie dla podłączonych dysków sieciowych NAS.
19. Ochrona przed niebezpiecznymi rodzajami aktywności sieciowej i atakami, możliwość tworzenia reguł wykluczających dla określonych adresów/zakresów IP.
20. Program musi posiadać możliwość zdefiniowania reguł dla rejestru systemu, procesów, aplikacji i plików. Program musi wykryć infekcje mające na celu zmniejszenie wydajności systemu operacyjnego.
21. Program musi chronić przed stronami internetowymi, które podszywają się pod zaufane serwisy WWW i próbują zdobyć poufne informacje.
22. Program musi kontrolować urządzenia i blokować nieautoryzowane nośniki danych. Program daje możliwość tworzenia reguł w oparciu o grupy użytkowników w celu dopasowania do polityki bezpieczeństwa.
23. Centralne zbieranie i przetwarzanie alarmów w czasie rzeczywistym.

**Wymagania techniczne dla konsoli do centralnego zarządzania oprogramowaniem antywirusowym:**

1. Obsługa serwerów baz danych:
   1. Microsoft SQL Server 2008, 2008 R2, 2012, 2014, 2016 i 2017
   2. MySQL
2. Za pomocą konsoli możliwa będzie zdalna instalacja oprogramowania na stacjach roboczych, urządzeniach mobilnych i serwerach oraz pełny podgląd stanu ochrony sieci dla wszystkich 200 licencji.
3. Obsługa komunikacji z agentami i gromadzenie danych aplikacji oraz przechowywanie ich w bazie danych.
4. Możliwość tworzenia raportów o stanie sieci w oparciu o minimum 1000 zmiennych.
5. Możliwość konfiguracji automatycznego generowania i wysłania raportu na konkretny adres e-mail według ustalonego harmonogramu, w określonych interwałach.
6. Możliwość skonfigurowania za pomocą konsoli powiadomienia poprzez widomość e-mail o wykrytym nowym zagrożeniu na stacji roboczej lub serwerze.
7. Za pomocą konsoli możliwe będzie tworzenie wyjątków oraz przesłanie plików do dalszej analizy.
8. Konsola musi posiadać funkcję gromadzenia danych sprzętu z połączonych urządzeń, m.in. informacji o pamięci RAM, pamięci masowej i procesorach.
9. Konsola musi posiadać funkcję filtrowania połączonych urządzeń w oparciu o ich parametry sprzętowe.
10. Możliwość wyboru pozycji z kategorii spisu sprzętu: obudowa, informacje o urządzeniu, ekran, układ graficzny, urządzenie wejściowe, pamięć masowa, układ sieciowy, drukarka, procesor, pamięć RAM i układ dźwiękowy.
11. Możliwość z poziomu konsoli: aktualizacji wszystkich modułów produktu zabezpieczającego zainstalowanego na docelowym urządzeniu, uruchomienie skanowania na żądanie, wykonanie określonych instrukcji wiersza polecenia na stacji roboczej lub serwerze.
12. Za pomocą konsoli możliwość deinstalacji aplikacji lub programu zainstalowanego na stacji roboczej, serwerze.

**Dodatkowe uwagi:**

1. Zamawiający nie dopuszcza poniesienia żadnych dodatkowych kosztów z tytułu zakupu jakichkolwiek dodatkowych licencji lub związanych z modyfikacją czy też zmianą konfiguracji działającego w firmie oprogramowania, jak również oprogramowania oczekiwanych przez Zamawiającego funkcjonalności dostarczanego przez Wykonawcę programu.
2. Wszystkie parametry i opis funkcji muszą być potwierdzone dokumentacją producenta przedstawioną przez Wykonawcę na każde żądanie Zamawiającego.
3. Dostawa obejmuje dokumenty i kody licencyjne (jeśli dotyczy) wraz z niezbędnymi nośnikami oprogramowania, lub wskazuje alternatywny sposób dostarczenia oprogramowania, umożliwiający Zamawiającemu korzystanie z pełni jego funkcjonalności.
4. Wykonawca w ramach realizacji umowy odinstaluje posiadane przez Zamawiającego oprogramowanie antywirusowe, dokona instalacji i uruchomienia dostarczonego oprogramowania w jednostkach Zamawiającego znajdujących się w budynkach Zamawiającego, w pomieszczeniach przez niego wskazanych.
5. Wykonawca musi odinstalować użytkowane przez Zamawiającego oprogramowanie antywirusowe przed instalacją i aktywacją dostarczonego oprogramowania antywirusowego.
6. W przypadku odinstalowania istniejącego na komputerach Zamawiającego oprogramowania antywirusowego i instalacji dostarczanego oprogramowania antywirusowego, musi ono być aktywne i w pełni funkcjonalne w dniu jego instalacji.

**Załącznik nr 4 –** Formularz ofertowy do postępowania

(wypełnia wykonawca )

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Część I**

**Zakup i dostawa dwóch klastrów urządzeń klasy UTM**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Część II**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam, że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Zakup i dostawa macierzy flash - 1 szt**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – dla każdego z ww. przedmiotów zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Część III**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Przedłużenie usługi wsparcia technicznego producenta na kolejny rok dla infrastruktury macierzy dyskowych posiadanych przez Zamawiającego**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Część IV**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Zakup i dostawa dysku zewnętrznego – 1 szt.**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Część V**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Dostawa oprogramowania serwerowego Windows Server Standard Core 2 SL lub równoważnego wraz z licencjami dostępowymi Windows Server User CAL lub równoważnymi**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Część VI**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Zakup oprogramowania do obróbki graficznej CorelDRAW Graphics Suite 2020 lub równoważnego**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

**Część VII**

Oferuję Zamawiającemu - Sieci Badawczej Łukasiewicz – Krakowskiemu Instytutowi Technologicznemu podany niżej przedmiot zamówienia

oraz oświadczam że zaoferowany przeze mnie przedmiot zamówienia spełnia wymagania opisu technicznego zawartego w SIWZ w tym zwłaszcza zał. Nr 3 do SIWZ

**Zwiększenie  o 150 stanowisk  licencji  na posiadane przez Zamawiającego  oprogramowanie antywirusowe ESET Endpoint Antivirus Suite**

|  |  |
| --- | --- |
| Nazwa własna urządzenia/oprogramowania ( producent, typ, model ) – podać dla każdego ww. przedmiotu zamówienia | CENA  (z vat)  [PLN]  całości zamówienia |
|  |  |

**Uwaga:** Zamawiający żąda wskazania przez wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podania przez wykonawcę firm podwykonawców

|  |  |
| --- | --- |
| Następującą część zamówienia zamierzam powierzyć podwykonawcy: | Nazwy firm podwykonawców: |
|  |  |

W przypadku braku takiego wskazania Zamawiający uzna, iż Wykonawca będzie realizował zamówienie bez udziału Podwykonawców

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

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

\* 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).

...................................... ..............................., dnia ….... –.............

Podpisy i pieczątki imienne osób

upoważnionych do reprezentowania Wykonawcy

1. Uczestnictwo w szkoleniu jest bezpłatne, nie wlicza się również w czas i zakres świadczenia usługi dla Instytutu [↑](#footnote-ref-1)