Kasa Rolniczego Ubezpieczenia Społecznego - CENTRALA
00 – 608 Warszawa, Al. Niepodległości 190

Biuro Zamówień Publicznych
tel.: (22) 592-64-20
e-mail:bzp@krus.gov.pl

Postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego

na zakup oprogramowania wspomagającego bezpieczeństwo

Specyfikacja istotnych warunków zamówienia
(zwana dalej SIWZ)

Rozdział I – Instrukcja dla Wykonawców
Rozdział II – Wzór umowy
Rozdział III – Formularz ofertowy i załączniki

Warszawa, 2017r.
0000-ZP.261.18.2017

Rozdział I – Instrukcja dla Wykonawców

1. Nazwa, adres Zamawiającego oraz tryb udzielenia zamówienia

Kasa Rolniczego Ubezpieczenia Społecznego – Centrala z siedzibą w Warszawie przy Al. Niepodległości 190, zwana dalej „Zamawiającym" lub „KRUS" ogłasza postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie art. 39 ustawy – Prawo zamówień publicznych z dnia 29 stycznia 2004r., zwanej dalej ustawą (Dz. U. z 2015r. poz. 2164 z późn. zm.) zgodnie z opisem przedmiotu zamówienia.

2. Opis przedmiotu zamówienia

2.1 Przedmiotem zamówienia jest :

a. Zakup tj. dostawa i wdrożenie oprogramowania wspomagającego bezpieczeństwo wraz z rocznym wsparciem technicznym producenta, w tym:

i. wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy producenta oferowanego rozwiązania..

ii. dostęp do nowych wersji oprogramowania, do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

b. świadczenie przez Wykonawcę, co najmniej 30 godzin konsultacji związanych z użytkowaniem oprogramowania (lub większej liczby godzin, zgodnie ze złożoną ofertą).

i. Usługi te będą świadczone co najmniej w dni robocze Zamawiającego, w godz. 7.00 – 17.00.

ii. Usługi świadczone będą przez Wykonawcę po zgłoszeniu potrzeby Zamawiającego do Wykonawcy na wskazany adres mail-owy. Wykonawca przedstawi Zamawiającemu do akceptacji liczbę godzin wymaganą do obsługi zgłoszenia.

c. świadczenie usługi audytu, raz w miesiącu, (usługa audytu nie wchodzi w zakres konsultacji opisanych w pkt 2.1 lit. b) systemu bezpieczeństwa firewall przez Wykonawcę, po dostarczeniu oraz wdrożeniu oferowanego systemu, która obejmować będzie:,

i. przygotowanie miesięcznych, cyklicznych raportów bezpieczeństwa z zakresu:

- incydentów związanych z wyciekiem informacji, wraz z komentarzem i zestawem rekomendacji, obejmujących w szczególności stosowną rekonfigurację obsługiwanego systemu,
- incydentów związanych z wykrytymi anomaliami sieciowymi, wraz z komentarzem i zestawem rekomendacji, obejmujących w szczególności stosowną rekonfigurację obsługiwanego systemu,

ii. analizę zidentyfikowanych incydentów bezpieczeństwa,

d. przeprowadzenie:

i. 2-dniowych warsztatów stacjonarnych, dla 4 pracowników Zamawiającego, w zakresie systemu zaawansowanej ochrony stacji użytkowników i serwerów,

ii. 3-dniowych warsztatów stacjonarnych, dla 4 pracowników Zamawiającego, w zakresie systemu bezpieczeństwa firewall.

2.2. Szczegółowy opis przedmiotu zamówienia zawarto we wzorze umowy – Rozdział II SIWZ załącznik nr 1 do Umowy.

2.3. Przedmiot zamówienia został określony wg kodów zawartych we Wspólnym Słowniku Zamówień (CPV): 48730000-4 – Pakiety oprogramowania zabezpieczającego.

3. Termin wykonania zamówienia

Wykonawca jest zobowiązany w terminie:

i. nie później niż 40 dni od dnia zawarcia umowy, wdrożyć oprogramowanie będące przedmiotem zamówienia,
ii. 1 roku od momentu wdrożenia oprogramowania, świadczyć usługi audytu systemu bezpieczeństwa firewall oraz konsultacji.

4. Warunki udziału w postępowaniu

4.1.O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

4.1.1. nie podlegają wykluczeniu na podstawie art. 24 ust. 1 ustawy;

W przypadku oferty składanej wspólnie przez kilku Wykonawców, ocena wymagań określonych w ppkt 4.1.1. będzie dla tych Wykonawców dokonana odrębnie.

4.1.2. spełniają warunki udziału w postępowaniu dotyczące:

4.1.2.1. kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie określa szczegółowego wymagania w tym zakresie.

4.1.2.2. sytuacji ekonomicznej lub finansowej – Zamawiający nie określa szczegółowego wymagania w tym zakresie.

4.1.2.3. zdolności technicznej lub zawodowej –

A. Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał co najmniej 2 projekty polegające na dostawie i implementacji systemu bezpieczeństwa sieciowego firewall o łącznej wartości nie mniejszej niż 150 tys. zł brutto.
Zamawiający dopuszcza, aby na spełnienie warunku Wykonawca wykazał dostarczone i wdrożone Projekty, które nadal utrzymuje.

B. Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże, że dysponuje lub będzie dysponował, przedstawiając jednocześnie informacje o podstawie dysponowania, osobami zdolnymi do wykonania zamówienia, legitymującymi się doświadczeniem i umiejętnościami odpowiednimi do funkcji, jakie zostaną im powierzone, spełniającymi niżej wymienione wymagania:

1. minimum 1 osobą do pełnienia funkcji Kierownika zespołu wdrożeniowego, która powinna się cechować następującymi kompetencjami:
   i. minimum 2-letnie doświadczenie w realizacji projektów bezpieczeństwa informatycznego,
   ii. kompetencje z obszaru bezpieczeństwa IT, w szczególności związane z technikami ofensywnymi oraz dobrymi praktykami wynikającymi z wiedzy audytorskiej (z uwagi na charakter poszukiwanego rozwiązania) potwierdzone co najmniej jednym z certyfikatatów: ISC2 CISSP, CISA, EC-Council Certified Ethical Hacker CEH, Offensive Security OSCP, Offensive Security OSCE lub równoważny do wymienionych;

2. minimum 2 osobami do pełnienia funkcji ekspertów bezpieczeństwa, certyfikowane w oferowanych technologiach lub posiadające inny dokument potwierdzający umiejętności takie jak potwierdza certyfikat, którzy będą uczestniczyć w implementacji rozwiązania oraz będą świadczyć usługę analizy incydentów bezpieczeństwa.

Ponadto,

i. za równoważne Zamawiający uzna certyfikaty, które potwierdzają co najmniej takie umiejętności jakie potwierdzają certyfikaty wymienione w wymaganiach dla danej osoby, wystawione przez podmiot, który na dzień publikacji ogłoszenia w niniejszym postępowaniu, prowadzi lub prowadził wcześniej działalność polegającą na certyfikowaniu tj. weryfikacji i potwierdzaniu umiejętności (wykluczone jest powoływanie się na certyfikaty lub dokumenty równoważne dla certyfikatów wydane przez Wykonawcę oraz podmioty z grupy kapitałowej Wykonawcy).
ii. w przypadku jeśli uzyskanie certyfikatu wymaga udziału w szkoleniu i/lub zdania egzaminu, Zamawiający za równoważny uzna certyfikat, którego wydanie poprzedzone zostało szkoleniem o co najmniej, jak dla wymaganego certyfikatu, okresie trwania i zakresie i/lub egzaminem o co najmniej, jak dla wymaganego certyfikatu, zakresie weryfikowanej wiedzy i kryteriach dla uzyskania pozytywnego wyniku,
iii. każda z powyższych funkcji (ról) musi być pełniona przez inną osobę,
iv. Wykonawca zapewni komunikację osób z Zamawiającym w języku polskim,
v. doświadczenie zawodowe uwzględniane będzie jedynie dla pełnych miesięcy kalendarzowych, przy czym czas doświadczenia nie będzie powiększany o czas pełnienia innych funkcji w projekcie lub pełnienia funkcji w innych projektach, w tym samym okresie.

<u>W przypadku oferty składanej wspólnie przez kilku Wykonawców, ocena wymagań określonych w pkt 4.1.2. będzie dla tych Wykonawców dokonana łącznie.</u>

4.2. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. W tym celu Wykonawca musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

4.3. Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1.

4.4. W celu oceny, czy Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Wykonawca zobowiązany będzie dołączyć do oferty dokumenty, które określają:

4.4.1. zakres dostępnych Wykonawcy zasobów innego podmiotu,

4.4.2. sposób wykorzystania zasobów innego podmiotu, przez Wykonawcę, przy wykonywaniu zamówienia publicznego,
4.4.3. zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego,
4.4.4. czy podmiot, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.

5. Wykaz oświadczeń i dokumentów potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia

5.1. Wykonawca zobowiązany jest dołączyć do oferty aktualne na dzień składania ofert oświadczenie własne (wzór oświadczenia stanowi załącznik nr 1 do SIWZ). Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

5.1.1. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, zamieszcza informacje o tych podmiotach w ww. oświadczeniu.

5.1.2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, ww. oświadczenie składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie to musi potwierdzać spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

5.2. Zamawiający, zgodnie z art. 24aa ust. 1 ustawy, najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. W tym celu, zgodnie z art. 26 ust. 1 ustawy, Zamawiający przed udzieleniem zamówienia wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni terminie, aktualnych na dzień złożenia oświadczeń i dokumentów, o których mowa w pkt 5.3. i 5.8.

5.3. **Na potwierdzenie nie podlegania wykluczeniu z postępowania Zamawiający będzie żądał od Wykonawcy, którego oferta zostanie najwyżej oceniona, następujących dokumentów:**

Zamawiający nie żąda dokumentów.

5.4. **Dokumenty podmiotów zagranicznych**

Zamawiający nie żąda dokumentów.

5.5. **Dokumenty dotyczące przynależności do tej samej grupy kapitałowej**

Wykonawca, w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp, przekaże Zamawiającemu oświadczenie o przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007r. o ochronie konkurencji i konsumentów (wzór oświadczenia stanowi *Załącznik nr 2 do SIWZ*). 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 o udzielenie zamówienia.

5.6. Wykonawca w sytuacji zaistnienia podstaw do jego wykluczenia z postępowania na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16-20 ustawy – Pzp, 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, tzw. self-cleaning. Zamawiający rozpatrzy dowody wykazane wyżej i dokona ich oceny w świetle przesłanek wykluczenia Wykonawcy określonych w art. 24 ust. 1 pkt. 13 i 14 oraz 16- 20 ustawy.

5.7. Postanowienia określone w pkt 5.6. nie mają zastosowania wobec Wykonawcy będącego podmiotem zbiorowym, wobec którego orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia i nie upłynął określony w tym wyroku okres obowiązywania zakazu.

5.8. **Na potwierdzenie spełnienia warunków udziału w postępowaniu Zamawiający będzie żądał następujących dokumentów:**

5.8.1. **W zakresie warunku dotyczącego kompetencji lub uprawnień do prowadzenia określonej działalności:**
Zamawiający nie żąda dokumentów.

5.8.2. **W zakresie warunku dotyczącego sytuacji ekonomicznej lub finansowej:**
Zamawiający nie żąda dokumentów

5.8.3. **W zakresie warunku dotyczącego zdolności technicznej lub zawodowej:**

5.8.3.1. wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych dostaw, w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów określających czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnych charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy, w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. Wykaz powinien zawierać dostawy na potwierdzenie

spełnienia warunków udziału w niniejszym postępowaniu *(wzór wykazu stanowi Załącznik nr 3 do SIWZ).*

5.8.3.2. wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz o podstawie dysponowania tymi osobami *(wzór wykazu stanowi załącznik nr 4 do SIWZ).*

5.9. Wykonawca nie jest zobowiązany do złożenia oświadczeń lub dokumentów potwierdzających spełnianie warunków udziału w postępowaniu lub brak podstaw wykluczenia, jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352).

6. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami

6.1. Postępowanie o udzielenie zamówienia prowadzi się z zachowaniem formy pisemnej, w języku polskim.

6.2. Komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 z późn. zm.) lub za pośrednictwem faksu.

6.3. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje przy użyciu środków komunikacji elektronicznej lub za pośrednictwem faksu, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt ich otrzymania.

6.4. W przypadku nie potwierdzenia ze strony Wykonawcy odbioru przesłanych informacji, Zamawiający uzna, że wiadomość dotarła do Wykonawcy po wydrukowaniu prawidłowego komunikatu poczty elektronicznej lub raportu z faksu o dostarczeniu informacji.

6.5. Postępowanie prowadzi Biuro Zamówień Publicznych. Wszelką korespondencję należy przesyłać na adres e-mail: bzp@krus.gov.pl lub pocztą na adres Al. Niepodległości 190, 00-608 Warszawa.

6.6. Uprawnionym ze strony Zamawiającego do porozumiewania się z Wykonawcami oraz udzielania wyjaśnień i informacji jest: Biuro Zamówień Publicznych tel. (22) 592-64-20 oraz fax. (22) 592-66-63, od poniedziałku do piątku w godz. 8:00 – 16:00.

7. Wymagania dotyczące wadium

7.1. Wykonawca jest zobowiązany do wniesienia wadium w wysokości: 7 000,00 zł (słownie: siedmiu tysięcy złotych) przed upływem terminu składania ofert, w jednej lub kilku z następujących form: pieniądzu, poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (j.t. Dz.U. 2014.1804 ze zm.). Wadium w pieniądzu należy wpłacić na rachunek bankowy Zamawiającego: **27 1130**

1017 0019 9015 9220 0003 z adnotacją *„Wadium na oprogramowanie wspomagające bezpieczeństwo.”*

7.2. W przypadku wadium wnoszonego w innych formach niż pieniądz, należy; oryginał dokumentu umieścić w odrębnej kopercie opatrzonej dopiskiem „WADIUM” i złożyć wraz z ofertą, natomiast kserokopię poświadczoną za zgodność z oryginałem dołączyć do oferty.

7.3. W przypadku wnoszenia wadium w formie gwarancji ubezpieczeniowej lub bankowej, gwarancja musi:

7.3.1. obejmować cały okres związania ofertą;

7.3.2. być samoistna, nieodwołalna, bezwarunkowa i płatna na pierwsze żądanie;

7.3.3. zawierać wszystkie przypadki utraty wadium, o których mowa w pkt 7.4 i 7.5;

7.3.4. podpisana przez upoważnionego przedstawiciela Gwaranta.

7.4. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 i 3a ustawy Pzp, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów, potwierdzających okoliczności, o których mowa w art. 25 ust. 1, oświadczenia, o których mowa w art. 25a ust. 1, pełnomocnictw lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3, co powodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej.

7.5. Zamawiający zatrzymuje wadium wraz z odsetkami w przypadku, gdy Wykonawca, którego oferta została wybrana:

7.5.1. odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie,

7.5.2. nie wniósł wymaganego zabezpieczenia należytego wykonania umowy,

7.5.3. zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

8. Termin związania ofertą

Termin związania ofertą wynosi **30 dni**.

Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

9. Opis sposobu przygotowywania ofert

9.1. Ofertę należy złożyć na Formularzu oferty wypełnionym wg wzoru zawartego w SIWZ, *Rozdział IV* – Formularz oferty i Załączniki do SIWZ,

9.2. Do oferty należy dołączyć pełnomocnictwo /upoważnienie/ do reprezentowania Wykonawcy w niniejszym postępowaniu, o ile oferta została podpisana przez osoby nie umocowane do tych czynności w dokumentach rejestracyjnych firmy (oryginał lub kopia poświadczona za zgodność z oryginałem przez notariusza) [pełnomocnictwo jest wymagane również, gdy ofertę składają podmioty występujące wspólnie (konsorcjum), a oferta nie jest podpisana przez wszystkich członków konsorcjum].

9.3. Zamawiający nie dopuszcza składania ofert częściowych

9.4. Zamawiający nie dopuszcza składania ofert wariantowych.

9.5. Zamawiający nie ujawnia informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. **Informacje zastrzeżone powinny być jednoznacznie oznaczone.**

9.6. Każdy Wykonawca może złożyć tylko jedną ofertę zawierającą jednoznacznie opisaną propozycję. Złożenie większej liczby ofert lub oferty zawierającej alternatywne propozycje spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
9.7. Oferta musi być sporządzona w języku polskim na maszynie, komputerze lub czytelną inną techniką w sposób zapewniający jej czytelność i podpisana przez osobę upoważnioną do reprezentowania Wykonawcy.
9.8. Oferta musi być podpisana przez osobę lub osoby upoważnione do reprezentowania Wykonawcy w sposób pozwalający na ich identyfikację (czytelny podpis lub imienna pieczątka). Zaleca się, aby wszystkie strony były parafowane przez osobę lub osoby upoważnione do reprezentowania Wykonawcy.
9.9. Ewentualne poprawki w ofercie powinny być naniesione czytelnie oraz opatrzone podpisem i pieczątką osoby upoważnionej do reprezentowania firmy.
9.10. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
9.11. Oświadczenia dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22a ustawy, składane są w oryginale.
9.12. Dokumenty, inne niż oświadczenia, o których mowa w pkt 9.11., składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem.
9.13. Poświadczenia dokumentów za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, w zakresie dokumentów, które każdego z nich dotyczą:
    9.13.1. poświadczenie za zgodność z oryginałem winno być sporządzone w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczątką osoby poświadczającej kopię dokumentu za zgodność z oryginałem);
    9.13.2. poświadczenie za zgodność z oryginałem następuje w formie pisemnej;
    9.13.3. w przypadku poświadczenia za zgodność z oryginałem dokumentów przez osobę/y, której/ych upoważnienie do reprezentacji nie wynika z dokumentu rejestracyjnego Wykonawcy, należy do oferty dołączyć oryginał stosownego pełnomocnictwa lub jego kserokopię, poświadczoną przez notariusza.
9.14. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

10. <u>Miejsce oraz termin składania i otwarcia ofert</u>

10.1. Ofertę należy złożyć w siedzibie Zamawiającego na adres: Al. Niepodległości 190, 00-608 Warszawa, pok. 101 – kancelaria lub drogą pocztową w terminie do dnia **31.08.2017r. do godz. 09:30** w zamkniętej kopercie z pieczątką Wykonawcy i oznaczonej w następujący sposób:

Kasa Rolniczego Ubezpieczenia Społecznego – Centrala - BZP
Al. Niepodległości 190, 00-608 Warszawa
„Oferta na zakup oprogramowania wspomagającego bezpieczeństwo”

10.2. Wykonawca może zmodyfikować lub wycofać ofertę pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie przed wyznaczonym terminem składania ofert.
10.3. Powiadomienie o modyfikacji oferty musi być złożone w zamkniętej kopercie oznaczonej pieczątką Wykonawcy i dopiskiem „Modyfikacja” .

10.4. W przypadku wycofania oferty, zgodnie z pkt 10.2, nie będzie ona otwierana i na wniosek Wykonawcy zostanie odesłana.
10.5. Koperty oznaczone dopiskiem „Modyfikacja" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i zostaną dołączone do oferty.
10.6. Zgłoszenia i pisma przesłane faksem nie będą traktowane jako oferty.
10.7. Otwarcie ofert nastąpi w dniu **31.08.2017r. o godz. 10:00** w siedzibie Zamawiającego w sali konferencyjnej „A" - parter.

11. Opis sposobu obliczenia ceny

11.1. Wykonawca określi ceny ściśle według zapisów zawartych w Formularzu oferty – *Rozdział III* SIWZ.
11.2. Cena musi być podana w złotych polskich (PLN) oraz wyrażona liczbowo i słownie, w zaokrągleniu do dwóch miejsc po przecinku (zgodnie z powszechnie przyjętym systemem rachunkowości).
11.3. Cena określona przez Wykonawcę powinna zawierać w sobie wszystkie koszty mogące powstać w okresie ważności umowy, a także uwzględniać inne opłaty i podatki wynikające z realizacji umowy, jak również ewentualne upusty i rabaty.
11.4. Stawka podatku VAT jest określona zgodnie z ustawą z dnia 11 marca 2004r. o podatku od towarów i usług (t.j. Dz.U. z 2016 r., poz. 710 z późn.zm.).
11.5. Cena podana w ofercie jest ostateczna i nie może ulec zmianie w trakcie realizacji umowy.
11.6. Zgodnie z art. 91 ust. 3a ustawy – Pzp, jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

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

12.1. Ocena ofert zostanie dokonana w oparciu o następujące kryteria wyboru:

Lp	Kryterium	Znaczenie w %	Opis
a)	Cena (Kc)*	60	Cena za wykonanie przedmiotu zamówienia (podana przez wykonawcę w zł brutto)
b)	Czas wdrożenia (Kw)	20	Proponowany termin wdrożenia oprogramowania (w pełnych dniach)
c)	Dodatkowe godziny konsultacji dla użytkownika (Kg)	20	Dodatkowe godziny konsultacji (pełne godziny) powyżej wymaganych przez Zamawiającego 30 godzin.

12.2. Kryteria będą wyliczone wg następujących zasad:

12.2.1. **Kryterium ceny (Kc)**

$$Kc = \frac{\text{Najniższa cena z ocenianych ofert}}{\text{Cena oferty ocenianej}} \times 60$$

Maksymalna liczba punktów jaką w tym kryterium otrzyma oferta wynosi **60**

12.2.2. **Kryterium czas wdrożenia oprogramowania** (**Kw**)
Zamawiający przyzna następującą liczbę punktów za termin wykonania zamówienia
40 dni – 0 pkt
35 dni – 5 pkt
30 dni – 10 pkt
25 dni – 20 pkt

Maksymalna liczba punktów jaką w tym kryterium otrzyma oferta wynosi **20.**

W przypadku zaoferowania przez Wykonawcę krótszego terminu niż 25 dni, ofercie zostanie przyznana maksymalna liczba 20 punktów.

12.2.3 **Kryterium liczby dodatkowych godzin konsultacji dla użytkownika (Kg)**
Zamawiający przyzna następująca liczbę punktów za dodatkowe godziny konsultacji dla użytkownika, realizowane w dni robocze Zamawiającego w godzinach od 7:00-17:00 przez zespół ekspertów bezpieczeństwa, o wymaganych w specyfikacji kompetencjach.

Za dodatkowe:
14 godzin – 4 pkt
28 godzin – 8 pkt
42 godziny –12 pkt
56 godzin – 16 pkt
70 godzin – 20 pkt

Maksymalna liczba punktów jaką w tym kryterium otrzyma oferta wynosi **20.**

W przypadku zaoferowania przez Wykonawcę większej liczby godzin konsultacji niż 70, ofercie zostanie przyznana maksymalna liczba 20 punktów.

12.3. Wskaźnik wynikowy (W) stanowi sumę punktów uzyskanych w obu kryteriach oceny ofert, wg wzoru: **W = Kc + Kw + Kg**, przy czym wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

13. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

13.1. Wykonawca przed podpisaniem umowy zobowiązany jest do:
13.1.1. Dostarczenia kopii potwierdzonych za zgodności z oryginałem wszystkich certyfikatów i zaświadczeń wskazanych w ofercie dotyczących osób wskazanych do realizacji zamówienia.
13.1.2. wniesienia zabezpieczenia należytego wykonania umowy zgodnie z pkt. 14 SIWZ.
13.2. Brak spełnienia wymogów określonych w pkt 13.1, w wyznaczonym przez Zamawiającego terminie, będzie jednoznaczny z odmową podpisania umowy przez Wykonawcę.

14. Wymagania dotyczące zabezpieczenia należytego wykonania umowy

14.1. Wybrany Wykonawca wniesie zabezpieczenie należytego wykonania umowy w wysokości 3 **%** ceny całkowitej brutto podanej w ofercie, najpóźniej w dniu podpisania umowy.

14.2. Zabezpieczenie może być wnoszone według wyboru Wykonawcy w jednej lub w kilku następujących formach:

14.2.1. pieniądzu;

14.2.2. poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;

14.2.3. gwarancjach bankowych;

14.2.4. gwarancjach ubezpieczeniowych;

14.2.5. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

14.3. Zabezpieczenie wnoszone w pieniądzu Wykonawca wpłaca przelewem na rachunek bankowy wskazany przez Zamawiającego.

14.4. W przypadku wnoszenia zabezpieczenia należytego wykonania umowy w formie gwarancji ubezpieczeniowej lub bankowej:

14.4.1. z jej treści winno wynikać, iż Gwarant gwarantuje nieodwołalnie i bezwarunkowo zapłatę wszelkich należności w wypadku niewykonania lub nienależytego wykonania umowy, w tym zapłatę należności z tytułu kar umownych na każde pisemne żądanie zgłoszone przez Zamawiającego (Beneficjenta).

14.4.2. winna być podpisana przez upoważnionego przedstawiciela Gwaranta.

14.5. Zamawiający zwolni zabezpieczenie należytego wykonania Umowy w wysokości 70% w terminie do 30 dni kalendarzowych od dnia wykonania przedmiotu Umowy i uznania przez Zamawiającego za należycie wykonane.

14.6. Kwota pozostawiona na zabezpieczenia roszczeń z tytułu rękojmi za wady zostanie zwrócona nie później niż w 15 dniu po upływie okresu rękojmi.

14.7. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone po potrąceniu przez Zamawiającego ewentualnych zobowiązań Wykonawcy względem Zamawiającego.

15. Wzór umowy

15.1. Umowa zostanie zawarta według wzoru zamieszczonego w SIWZ, Rozdział III – Wzór umowy.

15.2. Na podstawie art. 144 ust. 1 ustawy Zamawiający przewiduje możliwość zmiany postanowień zawartej umowy w stosunku do treści oferty.

15.3. Zamawiający przewiduje możliwość zmiany postanowień zawartej umowy na podstawie art. 142 ust. 5 ustawy Prawo zamówień publicznych

16. Informacja o podwykonawcach

16.1. Zamawiający dopuszcza udział podwykonawców w realizacji zamówienia.

16.2. Zamawiający żąda wskazania przez Wykonawcę części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez Wykonawcę firm podwykonawców.

16.3. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22a ust. 1, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać, że

proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

17. Informacja o przewidywanych zamówieniach

Zamawiający nie przewiduje możliwości udzielenia zamówień na podstawie art. 67 ust. 1 pkt 6) ustawy Pzp.

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

Wykonawcom, a także innym podmiotom, jeżeli mają lub mieli interes w uzyskaniu danego zamówienia oraz ponieśli lub mogą ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki odwoławcze zgodnie z działem VI – środki ochrony prawnej Prawa zamówień publicznych

Rozdział II – Wzór umowy

Umowa Nr ……

zawarta w Warszawie w dniu …….. roku pomiędzy: Skarbem Państwa - Kasą Rolniczego Ubezpieczenia Społecznego mającą siedzibę w Warszawie przy Al. Niepodległości 190, 00-608 Warszawa, NIP: 526-00-13-054, REGON: 012513262, reprezentowanym przez
Pana……..- Dyrektora Biura Informatyki i Telekomunikacji na podstawie pełnomocnictwa udzielonego przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego nr ……..…z dnia …….
zwaną dalej „Zamawiającym”,
a
firmą….....z siedzibą w ……., wpisana do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy…….pod numerem KRS:……., NIP: ……, o kapitale zakładowym:
lub (opcjonalnie):
……..., prowadzącym(ą) działalność gospodarczą pod nazwą ……..…… pod adresem……..., wpisanym(ą) do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, NIP**……,**REGON……..,

w imieniu której występuje:
……
Pana ……
zwanym dalej „Wykonawcą”,
zwanymi dalej łącznie Stronami

w wyniku przeprowadzenia postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie art. 39 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015r. poz. 2164 z późn. zm.) została zawarta umowa o następującej treści:

§ 1
PRZEDMIOT UMOWY

1. Przedmiotem umowy jest:
   a. zakup tj. dostawa i wdrożenie przez Wykonawcę oprogramowania wspomagającego bezpieczeństwo ……(*nazwa oprogramowania*) wraz z rocznym wsparciem technicznym producenta, w tym:
      i. wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy producenta oferowanego rozwiązania,
      ii. dostęp do nowych wersji oprogramowania, do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych,
   b. świadczenie przez Wykonawcę konsultacji związanych z użytkowaniem oprogramowania,
   c. po dostarczeniu oraz wdrożeniu zaoferowanego systemu, świadczenie przez Wykonawcę usługi audytu systemu bezpieczeństwa firewall,
   d. przeprowadzenie dla wyznaczonych pracowników Zamawiającego warsztatów stacjonarnych, o których mowa w § 3 ust. 5.
2. Szczegółowy opis przedmiotu umowy znajduje się w *Załączniku nr 1 do umowy.*

§ 2
TERMINY REALIZACJI UMOWY

1. Wykonawca zobowiązuje się:
   a. w terminie do dnia **……..** (*zostanie uzupełniony zgodnie z ofertą* dostarczyć i wdrożyć oprogramowanie, o którym mowa w § 1 ust. 1 lit. a umowy,
   b. nie później niż 10 dni po wdrożeniu systemu, przeprowadzić warsztaty, wskazane w § 3 ust. 5 umowy,
   c. w terminie 10 dni od dnia zakończenia wdrożenia, przekazać Zamawiającemu dokumentację powdrożeniową.
2. Potwierdzeniem wykonania dostawy i wdrożenia, przeprowadzenia warsztatów oraz przekazania dokumentacji, będzie podpisany bez zastrzeżeń przez przedstawicieli Zamawiającego i Wykonawcy protokół odbioru, którego wzór stanowi *Załącznik nr 2 do umowy.*
3. Usługi audytu systemu bezpieczeństwa firewall oraz konsultacji, o których mowa w § 1 ust. 1 lit. c i b umowy, będą świadczone przez okres 1 roku, od daty wdrożenia oprogramowania, zgodnie z ust. 1.

§ 3
ZASADY REALIZACJI UMOWY

1. W ramach wdrożenia, o którym mowa w § 1 ust. 1 lit. a. umowy, Wykonawca wykona i przeprowadzi:
   a) instalację i konfigurację oprogramowania,
   b) testy poprawności oprogramowania,
   c) konfigurację uprawnień dostępu,
   d) utworzenie polityk i reguł.
2. Prace polegające na instalacji, konfiguracji, testach i uruchomieniu realizowane będą w siedzibie Zamawiającego (budynek Centrali KRUS) – Warszawa, Al. Niepodległości 190 oraz w budynku dostawcy sieci WAN – Warszawa ul. Kaliska 11.
3. Wykonawca, w czasie trwania niniejszej umowy, zobowiązany będzie do świadczenia pomocy w ramach …….godz. konsultacji (*zgodnie ze złożoną ofertą*) dla użytkowników oprogramowania. Usługi te będą świadczone co najmniej w dni robocze Zamawiającego, w godzinach 07:00 – 17:00.
4. Usługi, o których mowa w ust. 3, świadczone będą przez Wykonawcę po zgłoszeniu potrzeby Zamawiającego do Wykonawcy na wskazany adres mail-owy. Wykonawca przedstawi Zamawiającemu do akceptacji liczbę godzin wymaganą do obsługi zgłoszenia.
5. W ramach umowy Wykonawca przeprowadzi w siedzibie Zamawiającego:
   a. 2-dniowe warsztaty stacjonarne dla 4 pracowników Zamawiającego, w zakresie systemu zaawansowanej ochrony stacji użytkowników i serwerów,
   b. 3-dniowe warsztaty stacjonarne, dla 4 pracowników Zamawiającego, w zakresie systemu bezpieczeństwa firewall.
6. Warsztaty, o których mowa w ust. 5 powinny być przeprowadzone przez certyfikowanego przedstawiciela producenta oprogramowania lub certyfikowanego konsultanta Wykonawcy.
7. Wykonawca w ostatnim dniu wdrożenia, przekaże Zamawiającemu:
   a. harmonogram warsztatów,
   b. program warsztatów wraz ze wskazaniem prowadzącego – do akceptacji Zamawiającego.
8. Wykonawca, w terminie określonym w § 2 ust. 1 lit. c przygotuje i przekaże Zamawiającemu dokumentację powdrożeniową.

9. Wykonawca, w czasie trwania niniejszej umowy, zobowiązany będzie do świadczenia raz w miesiącu usługi audytu systemu bezpieczeństwa sieciowego, która obejmować będzie:
   a. przygotowanie miesięcznych, cyklicznych raportów bezpieczeństwa z zakresu:
      i. incydentów związanych z wyciekiem informacji, wraz z komentarzem i zestawem rekomendacji, obejmujących w szczególności stosowną rekonfigurację obsługiwanego systemu,
      ii. incydentów związanych z wykrytymi anomaliami sieciowymi, wraz z komentarzem i zestawem rekomendacji, obejmujących w szczególności stosowna rekonfigurację obsługiwanego systemu.
   b. analizę zidentyfikowanych incydentów bezpieczeństwa.
10. Wykonawca, w terminie do 10 dnia każdego miesiąca, zobowiązany będzie do przygotowania, za poprzedni miesiąc, raportów, o których mowa w ust. 9.

§ 4
OBOWIĄZKI STRON

1. Wykonawca zobowiązuje się do:
   a) wykonywania usług wynikających z umowy w sposób jak najmniej uciążliwy dla Zamawiającego oraz dołożenia wszelkich starań w celu zminimalizowania czasu zatrzymania przetwarzania danych przez infrastrukturę użytkowaną przez Zamawiającego, natomiast jeśli konieczne będzie zatrzymanie przetwarzania, operacja zostanie wykonana w czasie dogodnym dla Zamawiającego,
   b) przestrzegania standardów i instrukcji wymaganych przez Zamawiającego i znanych Wykonawcy, w szczególności dotyczących bezpieczeństwa, ochrony poufności danych oraz mienia Zamawiającego,
   c) wykonywania usług pod nadzorem przedstawicieli Zamawiającego,
   d) współpracy z Zamawiającym w toku wykonywania przedmiotu umowy, w szczególności uwzględniania uwag zgłaszanych przez Zamawiającego w celu zapewnienia prawidłowej realizacji umowy,
   e) informowania Zamawiającego na każde jego żądanie o stanie zaawansowania prac związanych z realizacją przedmiotu umowy,
   f) ponoszenia odpowiedzialności za uszkodzenia produktów oraz infrastruktury Zamawiającego, bezpośrednio lub pośrednio spowodowanych działaniami lub zaniechaniami Wykonawcy,
   g) ponoszenia odpowiedzialności za działania lub zaniechania przedstawicieli Wykonawcy jak za swoje własne,
   h) skierowania do realizacji przedmiotu umowy pracowników posiadających doświadczenie w zakresie instalacji i wdrożeń oprogramowania, o którym mowa w § 1 ust. 1 lit. a. umowy. Skład zespołu Wykonawcy określa *Załącznik nr 3*. Wskazane osoby będą uczestniczyć we wdrożeniu rozwiązania oraz będą świadczyć usługę utrzymania oprogramowania i audytu incydentów bezpieczeństwa.
   i) każda zmiana w składzie zespołu Wykonawcy, o którym mowa powyżej, będzie wymagała uprzedniej zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności. W tym celu Wykonawca przedstawi propozycję zmiany wraz z uzasadnieniem, przy czym nie może mieć ona negatywnego wpływu na jakość świadczonych usług. Proponowane osoby muszą

posiadać co najmniej te same kwalifikacje, na które powoływał się Wykonawca w trakcie postępowania o udzielenie zamówienia.

Zamawiający ma prawo wystąpić do Wykonawcy z żądaniem odsunięcia danej osoby od realizacji umowy, jeżeli uważa, że osoba ta nie wywiązuje się należycie ze swoich obowiązków. Wykonawca zobowiązany jest zrealizować żądanie Zamawiającego niezwłocznie, nie później jednak niż w terminie określonym przez Zamawiającego.

Zmiana składu zespołu Wykonawcy nie stanowi zmiany umowy.

2. Do kontaktów w zakresie realizacji przedmiotu umowy Strony wyznaczają:
   a) ze strony Zamawiającego: ……, tel……adres e-mail…….
   b) ze strony Wykonawcy: ……., tel. ……., adres e-mail: ……
3. Zmiany personalne w zakresie, o którym mowa w ust. 2 nie wymagają zmiany umowy, a jedynie pisemnego powiadomienia drugiej Strony.
4. W czasie obowiązywania niniejszej umowy oraz przez czas nieograniczony po jej wygaśnięciu, Strony zobowiązane są zapewnić poufność informacji dotyczących drugiej Strony, w szczególności informacji technicznych, technologicznych, ekonomicznych, finansowych, handlowych, prawnych i organizacyjnych pozyskanych w związku z wykonywaniem niniejszej umowy i nie ujawniać tych informacji bez uprzedniej zgody drugiej Strony.
5. Żadna ze Stron nie będzie, bez uprzedniej pisemnej zgody drugiej Strony kopiować, rozpowszechniać ani ujawniać komukolwiek informacji dotyczących drugiej Strony, jej interesów, finansów lub działań, włącznie z wszelkimi informacjami technicznymi, finansowymi i tajemnicą przedsiębiorstwa, niezależnie od źródeł tych informacji, chyba, że taka informacja jest już powszechnie znana bez naruszenia postanowień niniejszej umowy lub musi być ujawniona uprawnionemu organowi lub osobom, działającym w ramach obowiązujących przepisów prawa.
6. Bez uprzedniej pisemnej zgody Zamawiającego, Wykonawca nie może przekazywać ani udostępniać osobom trzecim informacji, ani dokumentów związanych z realizacją niniejszej umowy, jak również wykonywanego przedmiotu niniejszej umowy, ani też wykorzystywać tychże informacji i dokumentów w interesie własnym, lub osób trzecich.

§ 5
PRAWA AUTORSKIE

1. Wykonawca gwarantuje, że realizacja niniejszej umowy nie spowoduje naruszenia czyichkolwiek praw autorskich, znaków handlowych, towarowych, patentów, rozwiązań konstrukcyjnych oraz innych praw chronionych.
2. Wykonawca przyjmuje na siebie wszelką odpowiedzialność za naruszenie praw osób trzecich w związku z realizacją Umowy, dotyczącą w szczególności naruszenia czyichkolwiek praw autorskich.
3. Z datą podpisania protokołu odbioru, na Zamawiającego przechodzą majątkowe prawa autorskie w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2016 r., poz. 666) do przekazanej dokumentacji powdrożeniowej, o której mowa w §3 ust. 8.
4. Na mocy niniejszej umowy Wykonawca udziela Zamawiającemu, na czas nieokreślony, prawa do korzystania z oprogramowania określonego w § 1 ust. 1 lit. a. umowy na następujących polach eksploatacji:
   a) prawo do korzystania z wszystkich funkcjonalności dostarczonego oprogramowania w dowolny sposób w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej

dla dostarczonego oprogramowania zgodnie z opublikowanymi przez producenta warunkami licencyjnymi,

b) prawo do instalowania dostarczonego oprogramowania w liczbie kopii/ stanowisk/ serwerów/użytkowników charakterystycznej dla dostarczonego oprogramowania zgodnie z opublikowanymi przez producenta warunkami licencyjnymi,

c) prawo do instalowania wszelkich poprawek opublikowanych na stronach producenta oprogramowania; oraz polach eksploatacji określonych w opublikowanych przez producenta warunkach licencyjnych.

§ 6
WYNAGRODZENIE

1. Całkowite wynagrodzenie Wykonawcy z tytułu realizacji przedmiotu umowy wynosi **……zł netto + 23% VAT, tj. …… zł brutto (słownie:** ……).
2. Wynagrodzenie, o którym mowa w ust. 1, obejmuje wszystkie elementy zamówienia, wymienione w § 1 ust. 1 umowy, oraz wynagrodzenie za przeniesienie praw, o których mowa w § 5 ust. 3 oraz udzielenie licencji w zakresie wskazanym w § 5 ust. 4. Wynagrodzenie to wyczerpuje wszelkie należności Wykonawcy związane z realizacją umowy i nie podlega zmianie w czasie trwania umowy, z zastrzeżeniem § 10 ust. 5 umowy.
3. Podstawą wystawienia przez Wykonawcę faktury VAT z tytułu realizacji niniejszej umowy będzie podpisany przez upoważnionych przedstawicieli Stron protokół odbioru bez zastrzeżeń.
4. Zapłata należności nastąpi na rachunek bankowy podany na fakturze, w terminie do 21 dni od dnia doręczenia do Zamawiającego oryginału prawidłowo wystawionej faktury VAT (wystawionej w PLN) wraz z protokołem odbioru, o którym mowa w ust. 3.
5. Za dzień zapłaty przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego należną Wykonawcy kwotą.

§ 7
KARY UMOWNE

1. W przypadku uchybienia określonemu w § 2 ust. 1 lit. a umowy terminowi wdrożenia oprogramowania, Wykonawca zapłaci Zamawiającemu karę w wysokości 2% wynagrodzenia całkowitego brutto określonego w § 6 ust. 1 umowy, za każdy dzień opóźnienia.
2. Wykonawca zapłaci Zamawiającemu karę umowną za odmowę lub nie udzielenie konsultacji, o której mowa w § 3 ust. 3, w wysokości 0,4% wynagrodzenia całkowitego brutto określonego w § 6 ust. 1 umowy, za każdy przypadek braku konsultacji.
3. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500,00 zł brutto za każdy dzień opóźnienia, w przypadku braku przygotowania miesięcznych, cyklicznych raportów z zakresu audytu systemu bezpieczeństwa sieciowego, w terminie wskazanym w § 3 ust. 10.
4. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500,00 zł brutto, w przypadku braku przygotowania i przekazania Zamawiającemu dokumentacji powdrożeniowej, w terminie wskazanym w § 2 ust. 1 lit.c).
5. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500,00 zł brutto, w przypadku nie przeprowadzenia warsztatów, w terminie wskazanym w § 2 ust. 1 lit.b).
6. W przypadku odstąpienia od umowy przez Wykonawcę lub Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia całkowitego brutto określonego w § 6 ust. 1 umowy.

7. Zamawiający może dochodzić odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych.
8. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującemu mu wynagrodzenia.

§ 8
ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

1. Wykonawca tytułem zabezpieczenia należytego wykonania umowy wniósł zabezpieczenie w wysokości **……** ceny całkowitej brutto podanej w ofercie, tj. w wysokości **…… zł (słownie:** ……..) w formie ……
2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
3. Zamawiający zwróci zabezpieczenie należytego wykonania umowy w wysokości 70% w terminie do 30 dni od dnia wykonania przedmiotu umowy i uznania przez Zamawiającego za należycie wykonane.
4. Kwota pozostawiona na zabezpieczenia roszczeń z tytułu rękojmi za wady zostanie zwrócona nie później niż w 15 dniu po upływie okresu rękojmi za wady.
5. Zabezpieczenie należytego wykonania umowy zostanie zwrócone po potrąceniu przez Zamawiającego ewentualnych zobowiązań Wykonawcy względem Zamawiającego.

§ 9

Podwykonawcy

(*zostanie uzupełnione opcjonalnie)*

(w przypadku gdy Wykonawca będzie korzystał z Podwykonawców)

1. Wykonawca w trakcie realizacji niniejszej umowy będzie korzystał z następujących Podwykonawców:
   a/ …….. w zakresie ……,
   b/ …….. w zakresie …….
2. Jeżeli w trakcie realizacji zamówienia nastąpi zmiana albo rezygnacja z podwykonawcy, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22a ust. 1 ustawy Prawo zamówień publicznych, w celu wykazania spełniania warunków udziału w postępowaniu lub kryteriów selekcji, o których mowa w SWIZ, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny podwykonawca lub wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.

(dotyczy przypadku, gdy Wykonawca nie korzysta z Podwykonawców)

Zgodnie z oświadczeniem złożonym w Formularzu ofertowym Wykonawca nie będzie korzystał z Podwykonawców.

§ 10
POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy ustawy Prawo zamówień publicznych, ustawy o prawie autorskim i prawach pokrewnych oraz ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2017r. poz. 459).
2. Oprócz przypadków przewidzianych w Kodeksie cywilnym, Zamawiający może odstąpić od niniejszej umowy w razie zaistnienia istotnej zmiany okoliczności, powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili jej zawarcia, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa

państwa lub bezpieczeństwu publicznemu - w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.

3. Zamawiający ma prawo odstąpić od umowy w trybie natychmiastowym w przypadku gdy Wykonawca nie wdroży oprogramowania o którym mowa w § 1 ust. 1 umowy, w terminie wskazanym w § 2 ust. 1 lit. a umowy.
4. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.
5. Zamawiający przewiduje możliwość zmiany postanowień niniejszej umowy w razie zaistnienia okoliczności, o których mowa w art. 142 ust. 5 ustawy Prawo zamówień publicznych. W takim przypadku wysokość wynagrodzenia, o którym mowa w § 6 ust. 1 umowy, ulegnie zmianie w następujący sposób:
   a) zmiana wysokości wynagrodzenia obowiązywać będzie od dnia wejścia w życie zmian, określonych w art. 142 ust. 5 ustawy Prawo zamówień publicznych,
   b) w przypadku zmiany stawki podatku od towarów i usług wartość netto wynagrodzenia Wykonawcy nie zmieni się, a określona w aneksie do umowy wartość brutto wynagrodzenia zostanie wyliczona na podstawie nowych przepisów,
   c) w przypadku zmiany wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, wynagrodzenie Wykonawcy ulegnie zmianie o wartość wzrostu całkowitego kosztu Wykonawcy wynikającą ze zwiększenia wynagrodzeń osób bezpośrednio wykonujących czynności przy realizacji przedmiotu umowy do wysokości aktualnie obowiązującego minimalnego wynagrodzenia, z uwzględnieniem wszystkich obciążeń publicznoprawnych od kwoty wzrostu minimalnego wynagrodzenia,
   d) w przypadku zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenie społeczne lub zdrowotne, wynagrodzenie Wykonawcy ulegnie zmianie o wartość wzrostu całkowitego kosztu Wykonawcy jaką będzie on zobowiązany dodatkowo ponieść w celu uwzględnienia tej zmiany, przy zachowaniu dotychczasowej kwoty netto wynagrodzenia osób bezpośrednio wykonujących czynności przy realizacji przedmiotu umowy,
   e) w przypadkach o których mowa w niniejszym ustępie lit. b)-d) wprowadzenie zmian wysokości wynagrodzenia wymaga uprzedniego złożenia wniosku dokumentującego wpływ zmian na koszty wykonania zamówienia przez Wykonawcę w terminie od dnia opublikowania przepisów dokonujących tych zmian do 30 dnia od dnia ich wejścia w życie,
   f) nie zawarcie w terminie jednego miesiąca od dnia złożenia wniosku o którym mowa w niniejszym ustępie lit. e) porozumienia w sprawie odpowiedniej zmiany wynagrodzenia uprawnia strony do rozwiązania umowy z zachowaniem trzymiesięcznego okresu wypowiedzenia, ze skutkiem nie wcześniejszym niż na koniec miesiąca,
   g) opisane powyżej zmiany wysokości wynagrodzenia dotyczą wyłącznie tej jego części, która będzie przysługiwać Wykonawcy za czynności wykonane po wprowadzeniu zmian, o których mowa w art. 142 ust. 5 ustawy Prawo zamówień publicznych.
6. Zamawiający nie wyraża zgody na cesję wierzytelności wynikających z realizacji niniejszej umowy.
7. Wszelkie ewentualne spory mogące powstać przy realizacji niniejszej umowy będą podlegały rozstrzygnięciu przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
8. Integralną część umowy stanowią wymienione w jej treści załączniki.

9. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednej dla każdej ze stron.

ZAMAWIAJĄCY: **WYKONAWCA:**

Wykaz załączników:
Załącznik nr 1 – Szczegółowy opis przedmiotu zamówienia
Załącznik nr 2 – Wzór protokołu odbioru
Załącznik nr 3 – Skład zespołu Wykonawcy.

Załącznik nr 1
do Umowy nr …..
z dn. ……..

Szczegółowy opis przedmiotu zamówienia

System zaawansowanej ochrony stacji użytkowników i serwerów wraz systemem bezpieczeństwa firewall

I. System ochrony stacji użytkowników i serwerów

Zamawiający wymaga dostarczenia rozwiązania do zaawansowanej ochrony stacji użytkowników oraz serwerów wraz ze wsparciem producenta na 1 rok według poniższych wymagań:

1 Wymagania funkcjonalne dla zaawansowanego systemu ochrony stacji końcowych użytkowników oraz serwerów

1.1 Oprogramowanie dla stacji końcowych i serwerów

1.1.1 Oferta powinna przedstawiać propozycję rozwiązania do ochrony co najmniej 250 stacji końcowych użytkowników i serwerów

1.1.2 Proponowane rozwiązanie powinno współegzystować z istniejącymi w organizacji rozwiązaniami zabezpieczeń stacji końcowych (np. AntyVirus, HIPS, itp.) w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwymi kodami wykonywalnymi.

1.2 Zarządzanie

1.2.1 Proponowane rozwiązanie powinno być zarządzane poprzez graficzny interfejs użytkownika typu Web (Web GUI).

1.2.2 Proponowane rozwiązanie powinno posiadać 3-warstwową architekturę składającą się z konsoli, serwera zarządzania oraz serwera bazy danych. Rozwiązanie powinno umożliwiać instalację i uruchomienia wszystkich trzech komponentów na jednym serwerze sprzętowym / wirtualnym lub instalację rozproszoną.

1.2.3 Proponowane rozwiązanie powinno umożliwiać instalację wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli.

1.2.4 Proponowane rozwiązanie powinno umożliwiać eksport logów w standardzie syslog do dowolnego zewnętrznego systemu zarządzania logów.

1.2.5 Proponowane rozwiązanie powinno być rozwiązaniem programowym działającym na systemie operacyjnym Windows Server.

1.2.6 Proponowane rozwiązanie powinno dawać możliwość uruchomienia w środowisku zwirtualizowanym (np. VMWare).

1.3 Zapobieganie atakom aplikacyjnym typu exploit.

1.3.1 Proponowane rozwiązanie powinno zapewniać ochronę procesów i aplikacji z możliwością dodawania do listy chronionych procesów aplikacji własnych.

1.3.2 Proponowane rozwiązanie powinno oferować funkcję monitorowania i uczenia się środowiska aplikacyjnego Zamawiającego (tj. rozpoznania procesów i aplikacji działających na stacjach końcowych użytkowników) celem uruchomienia wdrożenia pilotażowego.

1.3.3 Proponowane rozwiązanie powinno zapewniać ochronę w czasie rzeczywistym przed możliwością wykorzystania jakiegokolwiek błędu bezpieczeństwa aplikacji poprzez blokowanie technik wykonania ataku (technik "exploitacji").

1.3.4 Proponowane rozwiązanie powinno zapewniać poprzez blokowanie technik ataków skuteczną ochronę przed atakami wykonywanymi z użyciem exploit'ów dnia zerowego lub exploitów nieznanych wykorzystujących dowolny błąd bezpieczeństwa aplikacji.

1.3.5 Proponowane rozwiązanie powinno zapewniać możliwości monitorowania i zapobiegania atakom poprzez blokowania szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/lub usługi chmurowej i nie bazując na metodzie sygnaturowej.

1.3.6 W sytuacji wykrycia techniki ataku ukierunkowanej na podatną aplikację, celem zablokowania ataku proponowane rozwiązanie powinno zatrzymać proces atakowanej aplikacji, zebrać pełen zestaw danych dowodowych (takich jak nazwa atakowanego procesu, źródło pochodzenia pliku, znacznik czasowy, zrzut pamięci, wersja systemu operacyjnego, tożsamość użytkownika, wersja podatnej aplikacji, itp.) oraz zakończyć działanie tylko tego konkretnego procesu.

1.3.7 Proponowane rozwiązanie powinno wykorzystywać moduły zapobiegania i blokowania technik ataków. Jego działanie nie może być oparte o metodę sygnaturową, reputacyjną lub analizę heurystyczną pliku. Musi istnieć możliwość zastosowania modułów blokowania technik ataków zarówno dla powszechnie znanych i popularnych aplikacji jak również aplikacji własnych.

1.3.8 Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 1% a zajętość pamięci RAM nie więcej niż 20MB.

1.3.9 Proponowane rozwiązanie nie może stosować technik analizy exploit'ów wykorzystujących zasoby sprzętowe, takich jak lokalne środowisko symulacyjne typu "sandbox" lub zwirtualizowany kontener.

1.3.10 Proponowane rozwiązanie powinno aktualizować moduły blokowania technik ataków nie częściej niż raz na 6 miesięcy, tak aby minimalizować narzut czynności administracyjnych i operacyjnych związanych z aktualizacjami.

1.3.11 Proponowane rozwiązanie powinno umożliwiać jednoczesną ochronę wszystkich aplikacji i procesów przed wszystkimi technikami ataków.

1.3.12 Proponowane rozwiązanie powinno umożliwiać tworzenie wyjątków konfiguracyjnych dla określonych stacji końcowych i działających na nich procesów bezpośrednio z poziomu i na bazie zebranych po stronie konsoli zarządzającej logów.

1.4 Zapobieganie złośliwym plikom wykonywalnym

1.4.1 Proponowane rozwiązanie powinno zapewniać ochronę przed uruchomieniem złośliwych plików wykonywalnych.

1.4.2 Proponowane rozwiązanie powinno oferować funkcję monitorowania i uczenia się środowiska aplikacyjnego Zamawiającego (tj. rozpoznania procesów i aplikacji działających na stacjach końcowych użytkowników) celem uruchomienia wdrożenia pilotażowego.

1.4.3 Proponowane rozwiązanie powinno umożliwiać pełną kontrolę i ustalanie restrykcji parametrów i sposobu uruchamiania plików wykonywalnych (np. dozwolone foldery źródłowe, ścieżki sieciowe, urządzenia zewnętrzne, możliwość uruchamianie plików nie posiadających podpisu cyfrowego wystawcy, możliwość tworzenia procesów potomnych, itp.)

1.4.4 Proponowane rozwiązanie powinno umożliwiać zapobieganie uruchamianiu złośliwego oprogramowania poprzez użycie modułów blokujących typowe zachowania złośliwych kodów wykonywalnych.

1.4.5 Proponowane rozwiązanie powinno umożliwiać konfigurację globalnych list dozwolonych plików wykonywalnych w ramach organizacji.

1.4.6 Proponowane rozwiązanie powinno umożliwiać tworzenie wyjątków konfiguracyjnych dla określonych stacji końcowych celem wykluczenia ich z ogólnych reguł ochrony bezpośrednio z poziomu i na bazie zebranych po stronie konsoli zarządzającej logów.

1.5 Wykrywania nieznanych złośliwych kodów wykonywalnych

1.5.1 Proponowane rozwiązanie powinno posiadać opcję integracji ze stosowanym w organizacji chmurowym środowiskiem wykrywania ataków typu APT (Advanced Persistent Threat). Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.

1.5.2 Proponowane rozwiązanie powinno posiadać możliwość weryfikacji w chmurowym środowisku anty-APT czy dany plik jest złośliwy, czy legalny na bazie skrótu cyfrowego pliku.

1.5.3 Proponowane rozwiązanie powinno posiadać możliwość wysłania poprzez serwer zarządzania potencjalnie złośliwego pliku do analizy w chmurowym środowisku anty-APT.

1.5.4 Proponowane rozwiązanie powinno posiadać możliwość wglądu w raport wynikowy analizy pliku w środowisku chmurowym anty-APT bezpośrednio z poziomu stacji zarządzania oprogramowaniem zabezpieczeń stacji końcowych.

1.5.5 Proponowane rozwiązanie nie powinno analizować w środowisku chmurowym plików, które były w nim analizowane uprzednio. Powinien działać mechanizm powiadamiania, iż dany plik był już wcześniej poddawany analizie.

1.5.6 Proponowane rozwiązanie powinno posiadać możliwość zapobiegania nieznanym złośliwym plikom wykonywalnym poprzez zastosowanie chmurowego środowiska anty-APT typu “sandbox”. Dodatkowo powinna istnieć możliwość przedstawienia wyniku analizy pliku wraz z pełnym raportem z analizy.

1.5.7 Proponowane rozwiązanie powinno posiadać możliwość ręcznego dostrojenia lub nadpisania werdyktu będącego wynikiem analizy w środowisku chmurowym dla konkretnego skrótu cyfrowego pliku.

1.5.8 Proponowane rozwiązanie powinno posiadać możliwość zablokowania uruchomienia pliku wykonywalnego jeśli skrót cyfrowy pliku jest nieznany, tj. plik ten nie był uprzednio analizowany w środowisku chmurowym anty-APT producenta.

1.5.9 Proponowane rozwiązanie powinno posiadać możliwość zablokowania uruchomienia pliku wykonywalnego jeśli stacja końcowa nie może skomunikować się z symulacyjnym środowiskiem chmurowym, a skrót cyfrowy pliku jest nieznany lokalnie w bazie serwera zarządzania

1.5.10 Proponowane rozwiązanie powinno posiadać możliwość uruchomienia analizy statycznej pliku opartej o algorytmy uczenia maszynowego w przypadku braku połączenia do symulacyjnego środowiska chmurowego.

1.6 Raportowanie

1.6.1 Proponowane rozwiązanie powinno posiadać wbudowane pulpity raportów (ang. Dashboard) do monitorowania poziomu i stanu bezpieczeństwa przedsiębiorstwa:

a. Pulpit Stanu Komponentów Systemu
b. Pulpit Zdarzeń Bezpieczeństwa
c. Pulpit Szczegółowego Dziennika Zagrożeń
d. Pulpit Szczegółowego Dziennika Błędów Bezpieczeństwa

1.6.2 Proponowane rozwiązanie powinno posiadać wbudowane pulpity raportów (ang. Dashboard) do monitorowania stanu poszczególnych stacji końcowych w przedsiębiorstwie:

a. Pulpit Szczegółowego Stanu/Statusu Stacji Końcowych
b. Pulpit Historii Reguł Bezpieczeństwa Stacji Końcowych
c. Pulpit Zmian Reguł Bezpieczeństwa Stacji Końcowych
d. Pulpit Historii Stanu Serwisu Stacji Końcowych

1.6.3 Proponowane rozwiązanie powinno wyświetlać informacje, za pomocą przeglądarki www, na temat wykrytych zagrożeń i złośliwego oprogramowania oraz umożliwiać eksport dziennika zdarzeń zagrożeń i stanu stacji końcowych w formacie CSV.

1.7 Dokumentacja dowodowa (Forensics)

1.7.1 Zaproponowane rozwiązanie powinno umożliwiać zbieranie dokumentacji dowodowej i danych ze stacji końcowych w jednym centralnym punkcie.

1.7.2 Zaproponowane rozwiązanie powinno umożliwiać zbieranie następujących informacji w celu przeprowadzenia późniejszej analizy:

i. Zrzut pamięci (Memory Dump)
ii. Otwarte pliki
iii. Załadowane moduły
iv. Otwarte URI
v. Procesy nadrzędne

1.7.3 Zaproponowane rozwiązanie powinno umożliwiać użycie usługi inteligentnego transferu w tle - BITS (Background Intelligence Transfer Service) przy wykorzystaniu przeglądarki web oraz umożliwiać przesyłanie danych powiązanych z dokumentacją dowodową za pomocą niewykorzystanego pasma sieciowego.

1.7.4 Zaproponowane rozwiązanie powinno dawać możliwość dostosowania polityk powiązanych z dokumentacją dowodową w ramach serwera zarządzającego, w celu zdefiniowania jaki typ danych powinien zostać zebrany w przypadku wystąpienia incydentu.

1.7.5 Zaproponowane rozwiązanie powinno mieć możliwość wyświetlenia wysokopoziomowych informacji systemowych na temat stacji końcowej po wykryciu zagrożenia oraz zapewnić możliwość zebrania danych odnoszących się do zastosowanego mechanizmu ochrony celem dalszej analizy i śledztwa.

1.7.6 Zaproponowane rozwiązanie powinno umożliwiać automatyczne tworzenie wyjątków odnośnie reguł oraz skrótów cyfrowych bezpośrednio z raportu dotyczącego wykrytego zagrożenia w celu umożliwienia uruchomienia danego procesu na poszczególnych stacjach końcowych.

Usługa wdrożenia

Wraz z systemem wymagane jest wykonanie usługi wdrożenia oraz przygotowanie dokumentacji powdrożeniowej w terminie 10 dni od zakończenia wdrożenia.

Warsztaty

Wykonawca przeprowadzi min. 2 dniowe warsztaty dla 4 pracowników wskazanych przez Zamawiającego. Warsztaty muszą być przeprowadzone przez certyfikowanego z oferowanej technologii inżyniera oraz pokrywać wszystkie niezbędne elementy, pozwalające na samodzielną administrację wdrożonym systemem.

Usługa wsparcia technicznego

Wraz z produktem wymagane jest dostarczenie wsparcia producenta na okres 1 roku. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.

II. System bezpieczeństwa firewall

1. System zabezpieczeń firewall musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2. System zabezpieczeń firewall nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
3. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 2 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 250 000 jednoczesnych połączeń.
4. System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 8 interfejsów optycznych SFP.
5. System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych.
6. System zabezpieczeń firewall musi móc pracować w różnych trybach (wymienionych w poprzednim punkcie) jednocześnie w pojedynczej logicznej instancji systemu zabezpieczeń (np. wirtualny system, wirtualna domena, itp.).
7. System zabezpieczeń firewall musi mieć możliwość pracy w trybie transparentnym L1 (bez konieczności nadawania adresu IP) oraz pozwalać na tworzenie transparentnych subinterfejsów, które będą obsługiwały ruch z wybranych vlanów lub podsieci IP.
8. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
9. System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tablica routingu

w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
10. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji.
11. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
12. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
13. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
14. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 2 Gbit/s.
15. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
16. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
17. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
18. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
19. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
20. System zabezpieczeń firewall musi posiadać możliwość definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi istnieć możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
21. System zabezpieczeń firewall musi umożliwiać wysyłanie do chmury wybranych plików z kodem wykonywalnym celem zbadania czy nie zawierają one kodu złośliwego. Rozwiązanie musi zapewniać możliwość konfiguracji jakie typy plików i jakiego pochodzenia będą poddawane analizie w chmurze.
22. System zabezpieczeń firewall musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
23. System zabezpieczeń firewall musi umożliwiać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
24. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np.

komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

25. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

26. System zabezpieczeń firewall musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

27. System zabezpieczeń firewall musi mieć możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) powinna precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

28. System zabezpieczeń firewall musi mieć możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia.

29. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.

30. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

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

32. System zabezpieczeń firewall musi posiadać możliwość automatycznego pobierania listy stron WWW z zewnętrznego systemu w określonych przedziałach czasu i używania ich w politykach bezpieczeństwa.

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

34. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

35. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania

na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
36. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
37. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
38. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
39. System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
40. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
41. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
42. System zabezpieczeń firewall musi posiadać funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem.
43. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
44. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
45. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
46. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
47. System zabezpieczeń w ramach funkcjonalności zestawiania połączeń VPN musi umożliwiać dokonywanie inspekcji stacji roboczej pod kątem zainstalowanych aktualizacji, baz sygnatur i innych parametrów.
48. System zabezpieczeń musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
49. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
50. System zabezpieczeń firewall musi umożliwiać integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk

bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
51. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
52. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
53. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
54. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS i Kerberos.
55. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
56. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
57. Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia.
58. System zabezpieczeń firewall musi posiadać możliwość konfigurowania różnych serwerów Syslog per polityka bezpieczeństwa.
59. System zabezpieczeń firewall musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
60. System zabezpieczeń firewall musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
61. System zabezpieczeń firewall musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
62. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
63. System zabezpieczeń firewall musi być dostarczony w postaci klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu (pochodzących od tego samego producenta) pracujących w trybie Active-Passive z możliwością realizacji trybu Active-Active.

Usługa wdrożenia
Wraz z systemem wymagane jest wykonanie usługi wdrożenia oraz przygotowanie dokumentacji powdrożeniowej w terminie 10 dni od zakończenia wdrożenia.

Warsztaty
Wykonawca przeprowadzi min. 3 dniowe warsztaty dla 4 pracowników wskazanych przez Zamawiającego. Warsztaty powinny zostać przeprowadzone przez certyfikowanego z oferowanej technologii inżyniera oraz pokrywać wszystkie niezbędne elementy, pozwalające na samodzielną administrację wdrożonym systemem.

Usługa wsparcia technicznego
Wraz z produktem wymagane jest dostarczenie wsparcia producenta na okres 1 roku. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.

.

Załącznik nr 2
do Umowy nr …..
z dn. ……..

Warszawa, dn. …….

Protokół odbioru

W dniu …….. w ramach realizacji umowy nr …….., w siedzibie Centrali KRUS w Warszawie Al. Niepodległości 190, dokonano odbioru wykonania prac: ……...……
…….....

Niniejszy Protokół odbioru jest podstawą do wystawienia rachunku za wykonaną usługę.

Opracowanie zostało przyjęte/nieprzyjęte***** - uwagi:
……...
……...
……...
……...

* - niepotrzebne skreślić

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 3
do Umowy nr …..
z dn. ……..

Skład zespołu Wykonawcy.

W skład zespołu realizującego przedmiotową umowę wchodzą następujące osoby:

……...
……...
……...
……...

.........., dn. ……. **WYKONAWCA**

Rozdział III – Formularz oferty i Załączniki do SIWZ

Formularz oferty

Nazwa (Firma) Wykonawcy
…….,
Adres siedziby
……,
Adres do korespondencji
……,
Osoba do kontaktów - ……;
Tel. - .....; fax - .....;
E-mail: .....;

1. Oferujemy *dostawę i wdrożenie oprogramowania wspomagającego bezpieczeństwo……(wpisać nazwę oferowanego oprogramowania)* na następujących warunkach:

   Wynagrodzenie całkowite za wykonanie całości przedmiotu zamówienia wynosi …….. PLN brutto (słownie:……..),

   Termin wykonania …….. (podać w dniach) (*minimalnie 25 dni, maksymalnie 40 dni. Należy podać konkretnie 40, 35, 30 lub 25 dni, zgodnie z pkt. 12.2.2. SIWZ Rozdział I***)**

   Liczba dodatkowych godzin konsultacji dla użytkownika ….. *(podać w godzinach) (w przedziale 0 – 70 godzin. Należy podać konkretnie 14, 28, 42, 56 lub 70 dodatkowych godzin zgodnie z pkt 12.2.3. SIWZ Rozdział I)*

2. Oświadczamy, że:
   2.1. złożona przez nas oferta ……. **(wpisać: powoduje lub nie powoduje)*** powstanie u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług dla:

   …….....
   (wskazać nazwę (rodzaj) towaru lub usługi)

   o wartości …… (wskazać wartość bez kwoty podatku).

   UWAGA!
   Mechanizm odwrotnego obciążenia polega na przeniesieniu obowiązku rozliczania podatku VAT z Wykonawcy na Zamawiającego, zgodnie z postanowieniami ustawy z dnia 11 marca 2004 roku o podatku od towarów i usług.

   2.2. oferowany przez nas przedmiot zamówienia spełnia wszystkie wymagania określone przez Zamawiającego w SIWZ i zobowiązujemy się zrealizować przedmiot zamówienia na warunkach określonych w SIWZ;
   2.3. podana wyżej cena jest ostateczna i zawiera wszystkie koszty Wykonawcy.
   2.4. akceptujemy warunki płatności określone we Wzorze umowy.

2.5. zapoznaliśmy się ze SIWZ, w tym z wzorem umowy, nie wnosimy zastrzeżeń i zobowiązujemy się do stosowania określonych warunków oraz w przypadku wyboru naszej oferty - do zawarcia umowy zgodnej ze złożoną ofertą oraz postanowieniami SIWZ, w miejscu i terminie wyznaczonym przez Zamawiającego;
2.6. uważamy się za związanych niniejszą ofertą na czas wskazany w SIWZ, tj. przez okres **30 dni** od upływu terminu składania ofert;
2.7. deklarujemy wniesienie zabezpieczenia należytego wykonania umowy w wysokości **3%** ceny całkowitej brutto podanej w ofercie,
2.8. należymy/nie należymy*do sektora małych lub średnich przedsiębiorców.

3. **Informacje o oświadczeniach lub dokumentach ogólnodostępnych:**
   a) Nazwa dokumentu/oświadczenia* ……
   Adres strony internetowej: ……
   b) Nazwa dokumentu/oświadczenia* ……
   Adres strony internetowej: ……
   c) Nazwa dokumentu/oświadczenia* ……
   Adres strony internetowej: ……

*** niepotrzebne skreślić**

..... , dnia ..... ……

/pieczęć i podpis osoby/osób upoważnionej/ych do reprezentowania Wykonawcy/

Załącznik nr 1 do SIWZ

……
(nazwa i adres Wykonawcy)

OŚWIADCZENIE

w postępowaniu o udzielenie zamówienia publicznego
w trybie przetargu nieograniczonego
na zakup oprogramowania wspomagającego bezpieczeństwo

Ja, niżej podpisany, reprezentując Wykonawcę, którego nazwa jest wskazana powyżej, jako upoważniony na piśmie lub wpisany w odpowiednich dokumentach rejestrowych, oświadczam, że:

1. Wykonawca ten spełnia warunki udziału w postępowaniu;
2. Wykonawca nie podlega wykluczeniu z postępowania;
3. Wykonawca powołuje się na zasoby następujących podmiotów:
   a) ……..(nazwa i adres podmiotu) w następującym zakresie …… (podać zakres w jakim wykonawca powołuje się na zasoby podmiotu),

   b) ……..(nazwa i adres podmiotu) w następującym zakresie …… (podać zakres w jakim wykonawca powołuje się na zasoby podmiotu),

   które to podmioty nie podlegają wykluczeniu z postępowania i spełniają warunki udziału w postępowaniu w ww. zakresie;

4. Wykonawca zamierza powierzyć wykonanie części zamówienia następującym podwykonawcom:
   c) ……..(nazwa i adres podwykonawcy) w następującym zakresie …… (podać część zamówienia, której wykonanie Wykonawca zamierza powierzyć podwykonawcy),

   d) ……..(nazwa i adres podwykonawcy) w następującym zakresie …… (podać część zamówienia, której wykonanie Wykonawca zamierza powierzyć podwykonawcy),

Miejscowość i data…….....

Podpis (imię, nazwisko)…….....

(*Podpis osoby lub osób uprawnionych do reprezentowania wykonawcy w dokumentach rejestrowych lub we właściwym pełnomocnictwie).*

Załącznik nr 2 do SIWZ

……
(nazwa i adres Wykonawcy)

OŚWIADCZENIE

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego: ……
ja, niżej podpisany, reprezentując firmę, której nazwa jest wskazana powyżej, jako upoważniony na piśmie lub wpisany w odpowiednich dokumentach rejestrowych, oświadczam, że:

1. *****nie należymy do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp.

2. *****należymy do grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp, w skład której wchodzą następujące podmioty:
    1. ……
    2. ……
    3. ……

Miejscowość ..... dnia .....

.....
(pieczęć i podpis osoby uprawnionej do
składania oświadczeń woli w imieniu Wykonawcy)

* - niepotrzebne skreślić

Załącznik nr 3 do SIWZ

……..
Pieczęć adresowa firmy Wykonawcy

Wykaz dostaw

Celem potwierdzenia spełnienia warunku udziału **w postępowaniu na zakup oprogramowania wspomagającego bezpieczeństwo,** określonego w pkt 4.1.2.3 SIWZ oświadczam, że zrealizowałem nw. dostawy wraz z wdrożeniem:

Lp.	Nazwa odbiorcy usługi	Nazwa oprogramowania	Okres świadczenia usługi		Wartość brutto
			od dnia	do dnia	
1					
2					
3					

W załączeniu dokumenty potwierdzające należyte wykonanie lub wykonywanie ww. zamówienia.

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

.....
/Podpis upoważnionego(ych) przedstawiciela(i) Wykonawcy/

Załącznik nr 4 do SIWZ

……..
Pieczęć adresowa firmy Wykonawcy

Wykaz osób

Przystępując do udziału w postępowaniu o zamówienie publiczne prowadzone w trybie przetargu nieograniczonego na **„zakup oprogramowania wspomagającego bezpieczeństwo”,** niniejszym wykazuję osoby posiadające stosowne kwalifikacje i uprawnienia, które będą uczestniczyć w wykonywaniu zamówienia.

Lp.	Rola/Funkcja	Imię i Nazwisko	Certyfikaty, dokumenty równoważne *	Doświadczenie	Informacja o podstawie dysponowania wykazanymi osobami
1.					
2.					
3.					

**W wykazie należy przedstawić szczegółowe informacje dotyczące przedstawianych kandydatów, wskazując w sposób precyzyjny i kompletny, które doświadczenia zawodowe dotyczą wymagań postawionych przez Zamawiającego, i w jakim zakresie, a także informacje dotyczące uzyskanych certyfikatów na potwierdzenie kompetencji zawodowych i doświadczenia.*

W wykazie należy przedstawić następujące informacje:

a) imię i nazwisko,
b) rola/funkcja w realizacji przedmiotu zamówienia,
   - posiadane uprawnienia w odniesieniu do każdego z wymaganych certyfikatów/dokumentów równoważnych:
     – datę i numer lub inne unikalne oznaczenie certyfikatu/dokumentu równoważnego,

- nazwę podmiotu wystawiającego,
- zakres uprawnień,

c) doświadczenie:
   - okres doświadczenia zawodowego;
   - nazwa zamówienia oraz na rzecz jakiego podmiotu była realizowana;
   - pełniona funkcja (rola) w ramach realizacji usługi;
   - okres pełnienia funkcji w wymaganym zakresie od do (dd/mm/rrrr);

d) informację o podstawie dysponowania daną osobą, np. poprzez użycie sformułowania "dysponują/dysponujemy osobą na podstawie ... (podać podstawę dysponowania osobą, np. umowa o dzieło, umowa o pracę, umowa zlecenia, lub inna umowa cywilno-prawna)" albo "będę/będziemy dysponować osobą na podstawie ... (podać podstawę dysponowania osobą, np. umowa o dzieło, umowa o pracę, umowa zlecenie, lub inna umowa cywilno-prawna)" – z wyłączeniem sytuacji, gdy dana osoba jest jednocześnie Wykonawcą (jako osoba fizyczna).

……..dn. ……..… ……

Podpis Wykonawcy