ZW.16.DOK.2019

ZAPYTANIE OFERTOWE

w postępowaniu o udzielenie zamówienia na:

dostawę licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz do ochrony urządzeń mobilnych na okres 36 miesięcy dla Agencji Rozwoju Pomorza S.A.

Kody CPV:

48760000-3 Pakiet oprogramowania do ochrony antywirusowej

Załączniki :

1. Formularz ofertowy – załącznik nr 1
2. Szczegółowa specyfikacja funkcjonalno-technicznych – załącznik nr 2
3. Wzór umowy – załącznik nr 3

ZAMAWIAJĄCY:

Agencja Rozwoju Pomorza S.A.
Al. Grunwaldzka 472 D
80-309 Gdańsk
KRS: 4441
NIP: 583-000-20-02
REGON: 190044530
Kapitał zakładowy: 26 320 000 PLN

TRYB UDZIELENIA ZAMÓWIENIA:

Postępowanie niniejsze prowadzone jest w trybie przetargu pisemnego na podstawie przepisów Kodeksu cywilnego, zgodnie z zasadą konkurencyjności zawartą w Wytycznych Ministerstwa Rozwoju w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020.

Do postępowania nie mają zastosowania przepisy ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2018 r., poz. 1986 ze zm.) na podstawie art. 4 pkt 8 tej ustawy.

§ 1

Opis, zakres przedmiotu zamówienia i termin realizacji zamówienia

1. Obecnie Agencja Rozwoju Pomorza S.A. posiada 140 licencji programu antywirusowego **ESET Endpoint Security Suite** oraz 30 licencji oprogramowania **ESET Endpoint Security for Mobile.**
2. Przedmiotem zamówienia jest dostawa 140 licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz 30 licencji oprogramowania do ochrony urządzeń mobilnych, na okres 36 miesięcy dla Agencji Rozwoju Pomorza S.A., w tym:
   a) dostarczenie Zamawiającemu licencji łącznie ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia, np. oryginalny nośnik, certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, jeśli jest to niezbędne dla nabycia przez Zamawiającego praw do tego oprogramowania lub jego uruchomienia,
   b) świadczenie bezpłatnych konsultacji telefonicznych w zakresie wsparcia technicznego przez Wykonawcę w godzinach pracy Zamawiającego, tj. od poniedziałku do piątku, w godz. 8.00 - 16.00 oraz dostępu do aktualizacji baz wirusów w okresie trwania przydzielonej licencji,
   c) nieodpłatne korzystanie z uaktualnień baz sygnatur wirusów,
   d) prawo do pobierania nieodpłatnie nowszych wersji oprogramowania w ramach dostarczonych licencji przez cały okres obowiązywania licencji,
   e) w przypadku zaistnienia takiej potrzeby, pełnej deinstalacji posiadanego przez Zamawiającego oprogramowania antywirusowego ze wszystkich stacji roboczych i serwerów Zamawiającego, łącznie z usunięciem wpisów w rejestrach systemowych przy jednoczesnym dokonaniu instalacji oferowanego oprogramowania antywirusowego na wszystkich stacjach roboczych i serwerach Zamawiającego,
   f) przeprowadzenie dedykowanego szkolenia dla 2 pracowników Zamawiającego w zakresie instalacji, konfiguracji, zarządzania, diagnostyki i rozwiązania problemów oferowanego oprogramowania antywirusowego,
   g) przeprowadzenia wymienionych działań w lit. e i f w godzinach pracy Zamawiającego, tj. od poniedziałku do piątku, w godz. 8.00 - 16.00.
3. **Program antywirusowy do ochrony stacji roboczych i serwerów oraz program antywirusowy do ochrony urządzeń mobilnych powinny być zarządzane przez jedną konsolę administracyjną.**
4. Szczegółowy opis przedmiotu zamówienia określony został w Szczegółowej specyfikacji funkcjonalno-technicznej – załącznik nr 2 do Zapytania ofertowego.
5. Zamawiający przewiduje zastosowanie prawa opcji polegającego na możliwości zakupu do 10 dodatkowych licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów (w okresie realizacji przedmiotu zamówienia).
6. Wykonawca zobowiązany będzie, w ramach zamówienia opcjonalnego, do dostarczenia dodatkowych licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów po cenie wskazanej w Formularzu ofertowym.
7. Zamawiający zastrzega, iż prawo opcji jest jego uprawnieniem, a nie obowiązkiem, co oznacza, że Wykonawcy nie przysługuje żadne roszczenie w przypadku nieskorzystania przez Zamawiającego z prawa opcji.
8. Zamawiający może skorzystać z prawa opcji w przypadku m.in. konieczności zwiększenia liczby użytkowników.
9. Zamawiający o konieczności skorzystania z prawa opcji powiadomi Wykonawcę, poprzez złożenie stosownego oświadczenia.

10. Miejsce dostawy – siedziba Zamawiającego w Gdańsku przy Al. Grunwaldzkiej 472 D, budynek Olivia Six.
11. Wykonawca zrealizuje zamówienie, w zakresie wskazanym w ust. 2, w terminie 3 dni roboczych od daty zawarcia umowy.

§ 2

Opis sposobu przygotowania oferty

1. Oferta powinna zostać sporządzona na Formularzu ofertowym wg wzoru stanowiącego załącznik nr 1 do Zapytania ofertowego.
2. Ofertę sporządza się w języku polskim z zachowaniem formy pisemnej pod rygorem nieważności. Wszystkie załączniki do oferty powinny być sporządzone w języku polskim.
3. Oferta wraz ze wszystkimi załącznikami musi być podpisana przez osobę/osoby upoważnione do reprezentowania Wykonawcy, zgodnie z wpisem do właściwego rejestru lub ewidencji działalności gospodarczej lub przez osobę umocowaną do podpisania oferty. Pełnomocnictwo powinno być dołączone do oferty, o ile nie wynika ono z innych załączonych dokumentów.
4. W przypadku braku pieczęci imiennej osoby podpisującej ofertę podpis musi być czytelny.
5. W przypadku, gdy Wykonawca dołącza do oferty kopię lub odpis dokumentu, powinny one być poświadczone za zgodność z oryginałem przez osobę/osoby upoważnione do reprezentowania Wykonawcy.
6. Wszystkie strony oferty wraz z załącznikami powinny być podpisane i ponumerowane.
7. Poprawki powinny być naniesione czytelnie i sygnowane podpisem przez osobę/osoby upoważnione do reprezentowania Wykonawcy.
8. Wykonawca winien umieścić ofertę w zamkniętej kopercie zaadresowanej **„Agencja Rozwoju Pomorza S.A., Al. Grunwaldzka 472 D, 80-309 Gdańsk”**. Oprócz nazwy i adresu Wykonawcy na kopercie należy umieścić napis:

   „Oferta na dostawę licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz do ochrony urządzeń mobilnych na okres 36 miesięcy dla Agencji Rozwoju Pomorza S.A. Nie otwierać przed 19 marca 2019 r., godz. 10:00”.

   Zamawiający nie ponosi odpowiedzialności za przypadkowe otwarcie oferty nie zabezpieczonej w powyższy sposób.
9. Wszystkie dokumenty załączone do oferty powinny być ważne w terminie składania ofert.
10. Wykonawca przed upływem terminu składania ofert, może wprowadzić zmiany do złożonej oferty. Wprowadzenie zmian do złożonych ofert należy dokonać w formie określonej w ust. 7 z dopiskiem „Zmiana oferty”.
11. Wykonawca przed upływem terminu składania ofert może wycofać swoją ofertę poprzez wysłanie informacji do Zamawiającego o wycofaniu swojej oferty, pod warunkiem, iż informacja ta dotrze do Zamawiającego przed upływem terminu składania ofert.
12. Oferta jest jawna od chwili jej otwarcia, z wyjątkiem informacji, które stanowią tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2018 r., poz. 419 ze zm.), co do których Wykonawca zastrzegł – nie później niż w terminie składania ofert – że nie mogą być udostępnione i muszą być oznaczone klauzulą „Tajemnica przedsiębiorstwa”. **Wykonawca zobowiązany jest wykazać, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.** Zaleca się, aby dokumenty te były spięte w sposób pozwalający na ich oddzielenie od reszty oferty.

13. Wykonawca ponosi koszty związane z przygotowaniem i złożeniem oferty.
14. Nie dopuszcza się składania ofert częściowych lub wariantowych.
15. Wykonawca ponosi wszelkie koszty związane z przygotowaniem oraz złożeniem oferty.
16. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

§ 3

Podmioty wykluczone z postępowania

1. Z postępowania wykluczeni są Wykonawcy, w odniesieniu do których wszczęto postępowanie upadłościowe lub których upadłość ogłoszono.
2. Z postępowania wykluczeni są Wykonawcy powiązani z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy, a Wykonawcą, polegające w szczególności na:
   a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
   b) posiadaniu co najmniej 5% udziałów lub akcji;
   c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
   d) pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze wykonawcy, w szczególności pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.
3. Ocena braku podstaw do wykluczenia Wykonawcy z postępowania nastąpi na podstawie dokumentów przedłożonych przez Wykonawcę w ofercie jak stanowi § 4.

§ 4

Dokumenty wymagane od Wykonawców w celu potwierdzenia braku podstaw do wykluczenia wykonawcy z postępowania

1. Wypełniony Formularz ofertowy – załącznik nr 1.
2. Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu. Jeżeli Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie złoży wymaganych pełnomocnictw, Zamawiający wezwie do ich złożenia, chyba że mimo ich złożenia oferta wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.
3. **W przypadku jeśli złożone dokumenty będą niezgodne z wymogami zapytania, wówczas oferta Wykonawcy zostanie odrzucona.**

§ 5

Sposób porozumiewania się Zamawiającego z Wykonawcami oraz tryb udzielania wyjaśnień

1. Do kontaktowania się z Wykonawcami (w dni robocze tj. od poniedziałku do piątku, w godz. 9.00 - 15.00) upoważnieni są: Adam Sieniawski - tel. 58 32 33 133, Marcin Hoppe – tel. 58 32 33 247, oraz kontakt mailowy: przetargi@arp.gda.pl
2. Każdy uczestnik postępowania ma prawo zwrócić się do Zamawiającego o wyjaśnienie treści niniejszego Zapytania ofertowego. Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później

niż na 2 dni przed upływem terminu składania ofert - pod warunkiem, że wniosek o wyjaśnienie treści Zapytania ofertowego wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

3. Jeżeli wniosek o wyjaśnienie treści Zapytania ofertowego wpłynął po upływie terminu składania wniosku, o którym mowa w punkcie poprzednim, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
4. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w pkt 2.
5. W uzasadnionych przypadkach, przed upływem terminu składania ofert, Zamawiający może zmienić treść Zapytania ofertowego. Dokonaną zmianę Zapytania ofertowego Zamawiający zamieści niezwłocznie na stronie, na której jest zamieszczone Zapytanie ofertowe.
6. Jeżeli w wyniku zmiany treści zapytania ofertowego będzie niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania i otwarcia ofert i zamieści informację na stronie, na której jest zamieszczone Zapytanie ofertowe.
7. Wszelkie pytania, wnioski, oświadczenia i informacje od Wykonawców powinny być formułowane na piśmie i przesłane pocztą na adres Zamawiającego lub faksem na nr (58) 32 33 200 lub w formie elektronicznej na adres e-mail: przetargi@arp.gda.pl
8. Wszelkie zawiadomienia, wnioski, oświadczenia i informacje oraz wyjaśnienia, odpowiedzi na pytania zamieszczane będą na stronie www.bip.arp.gda.pl, www.arp.gda.pl oraz powszechnie dostępnej stronie internetowej www.bazakonkurencyjnosci.funduszeeuropejskie.gov.pl.
9. Zamawiający poprawia w ofercie:
   a) oczywiste omyłki pisarskie,
   b) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   c) inne omyłki polegające na niezgodności oferty z Zapytaniem ofertowym, niepowodujące istotnych zmian w treści oferty

   - niezwłocznie zawiadamiając o tym wykonawcę, którego oferta została poprawiona.

§ 6

Składanie ofert

1. Oferty należy składać w siedzibie Agencji Rozwoju Pomorza S.A. przy Al. Grunwaldzkiej 472 D, w sekretariacie Zarządu – p. XIII (w dni robocze od poniedziałku do piątku w godz. od 8.00 do 16.00).
2. Termin składania ofert upływa dnia 19 marca 2019 r., o godz. 10.00.
3. Termin związania ofertą wynosi 30 dni od upływu terminu składania ofert.

§ 7

Kryteria wyboru oferty

1. Wszystkie oferty nie podlegające odrzuceniu oceniane będą na podstawie następujących kryteriów:

   Oferowana cena brutto – 100% (maksymalnie 100 punktów).

   C = [C_N / C_R] x 100

   C – ilość punktów dla kryterium „cena”

   C_N – najniższa oferowana cena

   C_R – cena oferty rozpatrywanej

2. Do oceny zostanie przyjęta wartości brutto przedstawiona w załączniku nr 1 do Zapytania ofertowego
3. Oferta musi zawierać cenę łączną, maksymalną i ostateczną, obejmującą wszystkie koszty Wykonawcy związane z realizacją przedmiotu zamówienia.
4. Cena oferty nie będzie podlegała zmianom przez cały okres realizacji przedmiotu zamówienia.
5. Za najkorzystniejszą zostanie uznana oferta Wykonawcy, która uzyska największą ilość punktów.
6. Cena musi być podana w złotych polskich.

§ 8

Zawarcie umowy

1. Wykonawca, którego oferta uznana zostanie za najkorzystniejszą, zobowiązany będzie do zawarcia umowy w terminie określonym przez Zamawiającego, nie później niż przed upływem terminu związania ofertą.
2. Warunki, na których będzie zawarta umowa określa załącznik nr 3 do Zapytania ofertowego.
3. Jeżeli Wykonawca, którego oferta została wyłoniona w niniejszym trybie będzie uchylał się od zawarcia umowy, Zamawiający wybierze ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny.

§ 9

Odrzucenie oferty i unieważnienie postępowania

1. Oferta wykonawcy zostanie odrzucona, jeżeli:
   a) będzie niezgodna z przepisami prawa;
   b) jej treść nie będzie odpowiadać treści niniejszego zapytania;
   c) jej złożenie stanowiło będzie czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
   d) zostanie złożona przez Wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia;
   e) zawiera błędy w obliczeniu ceny;
   f) zawiera omyłki rachunkowe w obliczeniu ceny, których nie można poprawić na zasadzie oczywistych omyłek rachunkowych bądź błędów rachunkowych;
   g) została złożona po wyznaczonym terminie.
2. Zamawiający unieważni niniejsze postępowanie o udzielenie zamówienia, jeżeli:
   a) nie złożono żadnej oferty nie podlegającej odrzuceniu;
   b) wystąpiła istotna zmiana okoliczności powodująca, że przeprowadzenie postępowania lub wykonanie zamówienia nie leży w interesie Zamawiającego;
   c) postępowanie obarczone jest niemożliwą do usunięcia wadą.
3. Zamawiający zastrzega sobie prawo unieważnienia niniejszego postępowania na każdym etapie bez podawania przyczyny.

§ 10

Właściwość prawa

W sprawach nie uregulowanych zastosowanie mieć będą powszechnie obowiązujące przepisy prawa polskiego.

§ 11

Informacje dodatkowe

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:
   a) administratorem danych osobowych jest Agencja Rozwoju Pomorza S.A., Al. Grunwaldzka 472 D, 80 - 309 Gdańsk, NIP 583 - 000 - 20 - 02, Regon 190044530, adres e-mail: sekretariat@arp.gda.pl, tel. +48 58 32 33 101, fax +48 58 32 33 200;
   b) inspektorem ochrony danych osobowych w Agencji Rozwoju Pomorza S.A. jest Lucjan Brudzyński, kontakt: rodo@arp.gda.pl;
   c) dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie niniejszego zamówienia prowadzonym w trybie Zapytania ofertowego;
   d) odbiorcami danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o przepisy ustawy o dostępie do informacji publicznej; oraz podmioty, z którymi Agencja Rozwoju Pomorza S.A. zawarła stosowne umowy powierzenia związane z przechowywaniem oraz certyfikowanym niszczeniem dokumentów;
   e) dane osobowe będą przetwarzane w związku z realizacją projektów współfinansowanych ze środków Unii Europejskiej w ramach programów krajowych i międzynarodowych realizowanych przez Agencję Rozwoju Pomorza S.A do upływu terminów wynikających z zawartych umów, jednak nie krócej niż do dnia 31 grudnia 2028 r.,
   f) obowiązek podania danych osobowych bezpośrednio dotyczących wykonawcy będącego osobą fizyczną jest niezbędny w celu udziału w niniejszym postępowaniu oraz w celu zawarcia i realizacji umowy;
   g) w odniesieniu do danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
   h) osoba, której dane są przetwarzane, posiada:
      i. na podstawie art. 15 RODO prawo dostępu do danych osobowych jej dotyczących,
      ii. na podstawie art. 16 RODO prawo do sprostowania jej danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w zakresie niezgodnym z zapytaniem ofertowym oraz nie może naruszać integralności protokołu oraz jego załączników),
      iii. na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (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),
      iv. prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych narusza przepisy RODO;
   i) osoba, której dane są przetwarzane, nie posiada:
      i. w związku z art. 17 ust. 3 lit. b, d lub e RODO prawa do usunięcia danych osobowych,

ii. prawa do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
iii. na podstawie art. 21 RODO prawa sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. c RODO.

2. Zamawiający informuje, iż przedmiotowe zamówienie będzie współfinansowane ze środków Unii Europejskiej w ramach programów krajowych i międzynarodowych realizowanych przez Agencję Rozwoju Pomorza S.A., w szczególności:
   a) Europejskiego Funduszu Rozwoju Regionalnego w ramach pomocy technicznej Programu Operacyjnego Inteligentny Rozwój;
   b) Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Pomorskiego na lata 2014 - 2020, projekt pt. „Pomorski Broker Eksportowy. Kompleksowy system wspierania eksportu w województwie pomorskim" oraz projekt pt. „Invest in Pomerania 2020";
   c) Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Pomorskiego na lata 2014 – 2020, projekt pt. „Pomorzanki w Biznesie";
   d) Funduszu Spójności w ramach Programu Operacyjnego Pomoc Techniczna 2014 – 2020;
   e) Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Europejskiej Współpracy Terytorialnej „Interreg Południowy Bałtyk", projekt pt. „Circular economy tools to support innovation in green and blue tourism SMEs (CIRTOINNO)" oraz projekt "Wellbeing Tourism in the South Baltic Region - Guidelines for good practices & Promotion (SBWELL)";
   f) Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Europejskiej Współpracy Terytorialnej „Interreg Europa", projekt pt. „Everywhere International SMEs (EIS)";
   g) Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Europejskiej Współpracy Terytorialnej „Region Morza Bałtyckiego 2014-2020", projekt pt. „Supporting Non-technological Innovation in Owner-managed Manufacturing SMEs through increased capacity of business intermediaries (SNOwMan)".

Nr sprawy ZW.16.DOK.2019 ***Załącznik nr 1 do Zapytania ofertowego***

FORMULARZ OFERTOWY

Zamawiający:
Agencja Rozwoju Pomorza S.A.
Al. Grunwaldzka 472 D
80-309 Gdańsk

w postępowaniu
na dostawę licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz do ochrony urządzeń mobilnych na okres 36 miesięcy dla Agencji Rozwoju Pomorza S.A.

A. DANE WYKONAWCY:

Wykonawca/Wykonawcy:……

……

Adres: ……

Osoba odpowiedzialna za kontakty z Zamawiającym:

……

Dane teleadresowe. na które należy przekazywać korespondencję związaną z niniejszym postępowaniem:
faks……

e-mail ……

Adres do korespondencji (jeżeli inny niż adres siedziby):

……

B. ŁĄCZNA CENA OFERTOWA BRUTTO:

Niniejszym oferuję/oferujemy realizację przedmiotu zamówienia według następujących cen:

Lp.	**Przedmiot zamówienia**	**Nazwa oferowanego przedmiotu zamówienia**	**Ilość wraz z prawem opcji**	**Cena jednostkowa netto w PLN**	**Wartość netto w PLN** *(kol. 4 x kol. 5)*	**Stawka podatku VAT**	**Wartość brutto w PLN**
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Oprogramowanie antywirusowe do ochrony stacji roboczych i serwerów		150				
2	Oprogramowanie antywirusowe do ochrony urządzeń mobilnych		30				
						ŁĄCZNA CENA BRUTTO OFERTY:	

ŁĄCZNA CENA OFERTOWA BRUTTO* PLN…… słownie ……..

* **ŁĄCZNA CENA OFERTOWA BRUTTO** stanowi całkowite wynagrodzenie Wykonawcy, uwzględniające wszystkie koszty związane z realizacją przedmiotu zamówienia.

C. OŚWIADCZAM, ŻE:

- wobec mnie/nas, jako Wykonawcy nie wszczęto postępowania upadłościowego lub nie znajduję/my się w stanie upadłości;
- nie jestem/jesteśmy powiązany/i osobowo lub kapitałowo z Agencją Rozwoju Pomorza S.A. lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Agencji Rozwoju Pomorza S.A lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy, w szczególności poprzez:
  a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
  b) posiadaniu co najmniej 5% udziałów lub akcji;
  c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
  d) pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze wykonawcy, w szczególności pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli.
- cena wskazana w ofercie obejmuje cały zakres przedmiotu zamówienia wskazanego przez Zamawiającego w Zapytaniu ofertowym, uwzględnia wszystkie wymagane opłaty i koszty niezbędne do zrealizowania całości przedmiotu zamówienia, bez względu na okoliczności i źródła ich powstania,
- zapoznałem/liśmy się ze szczegółowymi warunkami zawartymi w dokumentacji Zapytania ofertowego i przyjmuję/my je bez zastrzeżeń;
- zaoferowany przedmiot zamówienia spełnia minimalne wymagania wymienione w Szczegółowej specyfikacji funkcjonalno-technicznej stanowiącej załącznik nr 2 do Zapytania ofertowego
- wykonam/y zamówienie na warunkach i zasadach określonych przez Zamawiającego w Zapytaniu ofertowym;
- akceptuję/my wskazany w Zapytaniu ofertowym czas związania ofertą – 30 dni od upływu terminu składania ofert;
- w razie wybrania mojej/naszej oferty zobowiązuję/my się do podpisania umowy zgodnie ze wzorem, stanowiącym załącznik nr 3 do Zapytania ofertowego;
- zostałem/liśmy poinformowany, że mogę/możemy wydzielić z oferty informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji jednocześnie wykazując, iż zastrzeżone informację stanowią tajemnice przedsiębiorstwa oraz zastrzec w odniesieniu do tych informacji, aby nie były one udostępnione innym uczestnikom postępowania;
- oświadczam/y, że niniejsza oferta zawiera na stronach nr ..... informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji
- oświadczam/y, że wypełniłem/liśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, dalej RODO) - Dz. Urz. UE L 119 z 04.05.2016, str. 1, wobec osób fizycznych, od których dane osobowe bezpośrednio lub

pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia w niniejszym postępowaniu (w przypadku, gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczące lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO wykonawca **nie składa oświadczenia i wówczas treść oświadczenia należy przekreślić).**

D. SPIS TREŚCI:

Integralną część oferty stanowią następujące dokumenty:

1) ……;
2) ……;
3) ……;
4) ……;
5) ……;
6) ……

Oferta została złożona na ..... kolejno ponumerowanych stronach.

…….	…….
Pieczęć Wykonawcy	Data i podpis upoważnionego przedstawiciela Wykonawcy

ZW.16.DOK.2019 *Załącznik nr 2 do Zapytania ofertowego*

Szczegółowa specyfikacja funkcjonalno-techniczna

I. Dla oprogramowania antywirusowego do ochrony stacji roboczych i serwerów.

1. Pełne wsparcie dla systemu Windows Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10.
2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.
3. Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim.
4. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
10. Administrator ma możliwość dodania wykluczenia po tzw. HASH’u zagrożenia, wskazującego bezpośrednio na określoną infekcję, a nie konkretny plik.
11. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
12. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
13. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
14. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
15. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
16. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego).
17. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

18. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
19. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
20. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
21. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
22. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
23. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
24. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
25. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
26. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
27. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
28. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
29. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
30. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
31. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
32. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
33. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
35. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
36. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń

do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.

37. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
38. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
39. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
40. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
41. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
42. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
43. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
44. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
45. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
46. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
47. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
48. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
49. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
50. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http
51. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
52. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
53. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
54. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
55. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
56. W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji.
57. Aplikacja musi posiadać funkcję ręcznej aktualizacji komponentów programu.

58. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
59. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
60. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
61. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
62. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
63. Administrator ma możliwość dodania wykluczenia na podstawie procesu, wskazującego bezpośrednio na określony plik wykonywalny.
64. Program musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń zewnętrznych w zależności od zdefiniowanego przedziału czasowego.
65. Program musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”
66. Program musi posiadać system ochrony przed atakami sieciowymi (IDS).
67. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

Zapora osobista (personal firewall)

1. Zapora osobista ma pracować jednym z 4 trybów (automatyczny, interaktywny, oparty na regułach, uczenia się):
2. Program musi akceptować istniejące reguły w zaporze systemu Windows, zezwalające na ruch przychodzący
3. Możliwość tworzenia list sieci zaufanych.
4. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie
5. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
6. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet.
7. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
9. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu.
10. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
11. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci
12. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie.
13. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia.
14. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem.

Kontrola dostępu do stron internetowych

1. Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych.
2. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
3. Moduł musi posiadać także możliwość grupowania kategorii już istniejących.
4. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj.
5. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2008 R2, SBS 2011, Microsoft MultiPoint Server 2010.
2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
5. Wbudowana technologia do ochrony przed rootkitami i exploitami.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
8. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
9. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
10. Możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Skanowanie plików spakowanych i skompresowanych.
12. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
13. Aplikacja powinna wspierać mechanizm klastrowania.
14. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
15. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
16. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
17. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
18. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
19. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.
20. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
21. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
22. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
23. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.

24. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
25. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
26. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
27. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
28. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
29. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
30. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
31. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
32. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
33. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
34. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
35. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
36. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
37. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
38. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
39. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
40. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
41. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
42. Aplikacja musi wspierać skanowanie magazynu Hyper-V
43. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
44. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
45. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.

46. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
47. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
48. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
49. Program musi posiadać system ochrony przed atakami sieciowymi (IDS).
50. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2008 R2, 2012,2016 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance).
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Serwer administracyjny musi oferować możliwość wykorzystania silnika bazodanowego MS SQL lub MySQL, który został już wcześniej zainstalowany u zamawiającego w infrastrukturze.
5. Rozwiązanie ma być w pełni zgodne z rozporządzeniem RODO.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
9. Konsola musi umożliwiać zarządzanie wszystkimi rozwiązaniami Producenta zabezpieczającymi przed zagrożeniami.
10. Konsola musi umożliwiać zarządzanie systemem dynamicznej ochrony przed zagrożeniami
11. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
12. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
13. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
14. Komunikacja z konsolą powinna być zabezpieczona za pośrednictwem protokołu SSL.
15. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
16. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
17. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie „hardware fingerprint”
18. Serwer administracyjny musi oferować natywne wsparcie dla „VDI” oraz „Golden Master Image”
19. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
20. Rozwiązanie ma oferować możliwość komunikacji agenta przy wykorzystaniu http Proxy wbudowanego w serwer centralnego zarządzania bez wykorzystania dodatkowej maszyny Proxy
21. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
22. Serwer administracyjny musi oferować możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS
23. Serwer administracyjny musi oferować możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP

24. Serwer administracyjny musi oferować możliwość konfiguracji polityk zabezpieczeń takich jak ograniczenia funkcjonalności urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11
25. Serwer administracyjny musi oferować możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Map Google
26. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
27. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
28. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
29. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android oraz iOS.
30. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
31. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów bazowych zarządzanego komputera oraz weryfikację zainstalowanego oprogramowania firm trzecich na stacji dla systemów Windows, Mac oraz Linux z możliwością jego odinstalowania
32. Konsola ma oferować możliwość aktywacji oraz wdrożenie elementów systemu EDR producenta.
33. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
34. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
35. Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
36. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
37. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
38. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
39. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
40. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
41. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
42. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
43. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
44. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
45. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
46. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
47. Serwer administracyjny musi oferować możliwość utworzenia grup dynamicznych na podstawie zainstalowanego oprogramowania oraz zainstalowanych podzespołów bazowych w komputerach końcowych.

48. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, podzespoły bazowe itp.
49. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
50. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
51. Serwer administracyjny musi posiadać minimum 100 szablonów raportów przygotowanych przez producenta
52. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
53. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie danych z systemu EDR producenta
54. Serwer administracyjny musi oferować możliwość wygenerowania raportu na podstawie informacje o zainstalowanych podzespołów w stacjach roboczych
55. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
56. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
57. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
58. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień na zasadzie „WYSIWYG" z wykorzystaniem istniejących zmiennych
59. Powiadomienia mailowe mają być wysyłane w formacie HTML
60. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
61. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
62. Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
63. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
64. Rozwiązanie ma oferować weryfikację zainstalowanych komponentów bazowych urządzenia takich jak: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe, etc
65. Serwer administracyjny musi oferować aktualizację wszystkich komponentów z poziomu raportów jednym kliknięciem.
66. Rozwiązanie ma oferować instalację agenta rozwiązania DLP producenta z poziomu jednego repozytorium.
67. Serwer administracji musi umożliwić granulację uprawnień dla Administratorów w taki sposób, aby każdemu z nich możliwe było przyznanie oddzielnych uprawnień do poszczególnych grup komputerów, polityk lub zadań.
68. Konsola webowa musi umożliwiać zarządzanie systemem EDR producenta.
69. Administrator musi mieć możliwość podłączenia do stacji roboczej z użyciem protokołu RDP bezpośrednio z poziomu konsoli ERA.

70. Konsola administracyjna musi oferować możliwość weryfikacji zmian w produktach wprowadzanych przez producenta (Release notes dostępne bezpośrednio z konsoli zarzadzania)
71. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar
72. Musi istnieć mechanizm, umożliwiający dodawanie reguł do istniejących już w module firewalla lub harmonogramie. Takie reguły można umieścić na początku lub końcu istniejącej listy.
73. Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu interfejsu Konsoli administracyjnej.

II. Dla oprogramowania do ochrony urządzeń mobilnych

1. Wspierany system co najmniej Android 4.0 (Ice Cream Sandwich).
2. Rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Procesor: ARM (minimum ARMv7).
4. Pamięć wewnętrzna: 20 MB.
5. Połączenie z siecią Internet dla celów aktualizacji sygnatur i aktywacji licencji.

Ochrona antywirusowa:

1. Ochrona plików w czasie rzeczywistym.
2. Ochrona przed atakami typu „phishing".
3. Skanowanie rozszerzeń DEX, bibliotek SO plików archiwum oraz innych.
4. Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
5. Aplikacja musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
6. Ochrona proaktywna wykrywająca nieznane zagrożenia.
7. Aplikacja ma mieć możliwość określenia poziomu głębokości skanowania plików archiwum.
8. Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
9. W przypadku wykrycia zagrożenia użytkownik ma otrzymać odpowiednie powiadomienie.
10. Aplikacja musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia
11. Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności, w pełni naładowane i podłączone do ładowarki.

Skanowanie na żądanie:

1. Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji.
2. Aplikacja ma wykorzystywać do celu skanowania metody heurystyczne wykrywające nieznane zagrożenia.
3. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
4. Użytkownik ma mieć możliwość wskazania akcji jaka ma być podjęta w przypadku wykrycia zagrożenia: poddania kwarantannie, usunięcia lub zignorowania.
5. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany.
6. Aplikacja ma posiadać osobne dzienniki skanowania dla ochrony plików w czasie rzeczywistym, oraz skanowania na żądanie.
7. Reguły zdefiniowane przez administratora (w trybie administratora) muszą mieć wyższy priorytet niż reguły zdefiniowane przez użytkownika.
8. Użytkownik i administrator ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów.
9. Użytkownik i administrator ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla:
   a) Przychodzącej wiadomości SMS,
   b) Przychodzącej wiadomości MMS,

c) Połączenia wychodzącego,
d) Połączenia przychodzącego.

10. Aplikacja ma mieć możliwość aktywacji blokady dla wszystkich połączeń oraz wiadomości SMS/MMS dla znanych kontaktów znajdujących się w książce telefonicznej urządzenia.
11. Aplikacja ma mieć możliwość blokady połączeń telefonicznych oraz wiadomości SMS/MMS dla nieznanych kontaktów (nieznajdujących się w książce telefonicznej urządzenia).
12. Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).
13. Aplikacja ma być wyposażona w dziennik modułu antyspamowego zawierający informacje odnośnie filtrowania modułu.

Ochrona przed kradzieżą:

1. Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM.
2. Dodanie zaufanej karty SIM ma się odbyć się w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o dane wprowadzone ręcznie.
3. Wprowadzenie danych ręcznie dotyczących zaufanej karty SIM ma się odbywać w oparciu o numer IMSI karty SIM.
4. Aplikacja ma mieć możliwość wprowadzenia zaufanych odbiorców wiadomości, do których zostanie przesłana informacja w przypadku umieszczenia w urządzeniu innej niż zaufana karty SIM.
5. Aplikacja ma mieć możliwość włączenia opcji ignorowania niedopasowania kart SIM.
6. Użytkownik ma mieć możliwość edycji treści wiadomości SMS wysyłanej na zaufane numery telefonów w przypadku nie dopasowania karty SIM.
7. W przypadku kradzieży urządzenia, prawowity użytkownik ma mieć możliwość wysłania na urządzenie komendy która umożliwi:
   a) usunięcie zawartości urządzenia,
   b) zablokowania urządzenia,
   c) przesłania na zaufany numer telefonu lokalizacji GPS w której skradzione urządzenie się znajduje.
8. Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania.
9. Możliwość zdalnego zresetowania hasła ma być możliwa tylko w przypadku wysłania odpowiedniego polecenia z zaufanego urządzenia.

Polityka ustawień:

1. Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji czy są one zgodne z polityką.
2. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia:
   b) Połączenie Wi-Fi,
   c) Satelity GPS,
   d) Usługi lokalizacyjne,
   e) Pamięć,
   f) Roaming danych,
   g) Roaming połączeń,
   h) Nieznane źródła,
   i) Tryb debugowania,
   j) Komunikacja NFC,
   k) Szyfrowanie pamięci masowej.
3. Administrator ma mieć możliwość wyboru powyższych elementów.

Kontrola aplikacji:

1. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.
3. Blokowanie aplikacji musi być umożliwione co najmniej za pomocą polityk:
   a) manualnego zdefiniowania listy blokowanych aplikacji na podstawie nazwy,
   b) blokowanie na podstawie kategorii (np. kategorii Gry lub Społecznościowe),
   c) blokowanie na podstawie uprawnień aplikacji (np. aplikacji, które korzystają z modułu GPS do odczytania lokalizacji),
   d) blokowanie na podstawie źródła (np. aplikacje instalowane z innych źródeł niż sklep Google Play).
4. Administrator musi mieć możliwość monitorowania czasu, jaki użytkownik spędza na korzystaniu z poszczególnych aplikacji i sprawdzenia z jakich aplikacji użytkownik korzystał w ciągu ostatnich 30 dni, 7 dni oraz 24 godzin.

Zabezpieczenia urządzenia:

1. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
   a) minimalny poziom zabezpieczeń i złożoność blokady ekranu,
   b) maksymalną dopuszczaną liczbę błędnych prób odblokowania,
   c) odstęp czasu po którym użytkownik musi zmienić kod odblokowujący urządzenie,
   d) czas przeznaczony na odblokowanie urządzenia,
   e) ograniczyć dostęp do kamery wbudowanej w urządzenie.

Aktualizacje sygnatur:

1. Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
2. Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
3. Aplikacja ma mieć funkcjonalność ochrony hasłem wybranych modułów ochrony, w tym co najmniej dostępu do ustawień ochrony antywirusowej, ustawień modułu antyspamowego, ochrony przed kradzieżą, uruchamiania zadań audytu zabezpieczeń oraz przed deinstalacją.
4. Aplikacja ma mieć możliwość ukrycia ikony powiadomień.

Konfiguracja i zdalne zarządzanie:

1. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
2. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.
3. Administrator musi mieć możliwość zdalnego wysyłania komunikatów z poziomu konsoli centralnego zarządzania do użytkowników urządzeń mobilnych.
4. Przesłana wiadomość musi wyświetlać się w formie wyskakującego okna, aby użytkownik ich nie przeoczył.
5. Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania.

ZW.16.DOK.2019 *Załącznik nr 3 do Zapytania ofertowego*

Umowa nr _____

na dostawę licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz do ochrony urządzeń mobilnych na okres 36 miesięcy dla Agencji Rozwoju Pomorza S.A.

zawarta w Gdańsku dnia _____ 2019 roku, pomiędzy:

AGENCJĄ ROZWOJU POMORZA S.A. z siedzibą w Gdańsku przy Al. Grunwaldzkiej 472 D, wpisaną do rejestru przedsiębiorców prowadzonego przez, Sąd Rejonowy Gdańsk- Północ w Gdańsku, VII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000004441, kapitał zakładowy 26.320.000,00 PLN, reprezentowaną przez:

1.
2.

zwaną dalej „Zamawiającym”,

a

_____,

reprezentowaną przez:

1.

zwaną dalej “Wykonawcą”.

§ 1

1. Przedmiotem zamówienia jest dostawa 140 licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz 30 licencji oprogramowania do ochrony urządzeń mobilnych, na okres 36 miesięcy dla Agencji Rozwoju Pomorza S.A., zgodnie ze złożoną przez Wykonawcę w dniu _____ 2019 r. ofertą, stanowiącą załącznik nr 1 do umowy.
2. Zamawiający przewiduje zastosowanie prawa opcji polegającego na możliwości zakupu do 10 dodatkowych licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów. Skorzystanie z prawa opcji polegać będzie na złożeniu przez Zamawiającego, w okresie realizacji przedmiotu zamówienia, jednostronnego zamówienia określającego ilość dodatkowych licencji.
3. Wykonawca zobowiązany będzie, w ramach zamówienia opcjonalnego, do dostarczenia dodatkowych licencji oprogramowania antywirusowego do ochrony stacji roboczych i serwerów po cenie wskazanej w ofercie Wykonawcy w terminie 3 dni roboczych od daty otrzymania oświadczenia od Zamawiającego.
4. Zamawiający zastrzega, iż prawo opcji jest jego uprawnieniem, a nie obowiązkiem Zamawiającego, co oznacza, że Wykonawcy nie przysługuje żadne roszczenie w przypadku nieskorzystania przez Zamawiającego z prawa opcji.

5. Szczegółowy opis przedmiotu zamówienia zawarty jest w Zapytaniu ofertowym, stanowiącym załącznik nr 2 do umowy.
6. Wykonawca oświadcza, że korzystanie przez niego i przez Zamawiającego w szczególności z praw autorskich, licencji, praw własności przemysłowej, intelektualnej itp. nie narusza przepisów prawa, prawem chronionych dóbr osobistych lub majątkowych osób trzecich ani też praw na dobrach niematerialnych, w szczególności praw autorskich, praw pokrewnych, praw z rejestracji wzorów przemysłowych oraz praw ochronnych na znaki towarowe.

§ 2

1. Licencje oprogramowania antywirusowego do ochrony stacji roboczych i serwerów oraz licencje oprogramowania do ochrony urządzeń mobilnych zostaną udzielone na okres 36 miesięcy.
2. Wykonawca zobowiązuje się do wykonania przedmiotu umowy w terminie 3 dni roboczych od daty zawarcia umowy.
3. Po upływie okresu obowiązywania umowy, umowa ulega zakończeniu bez względu na stopień wykorzystania liczby licencji.
4. Wykonawca przejmuje na siebie wszelką odpowiedzialność z tytułu roszczeń, z jakimi osoby trzecie mogłyby wystąpić przeciwko Zamawiającemu z tytułu korzystania z należących do osób trzecich praw na dobrach niematerialnych, a w szczególności praw autorskich w odniesieniu do przedmiotu umowy.
5. Wykonawca zobowiązuje się do dostarczenia Zamawiającemu licencji łącznie ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia, np. oryginalny nośnik, certyfikat autentyczności, kod aktywacyjny oraz wraz z instrukcją aktywacji, jeśli jest to niezbędne dla nabycia przez Zamawiającego praw do tego oprogramowania lub jego uruchomienia.

§ 3

1. Zamawiający przewiduje przeznaczyć maksymalnie na realizację przedmiotu umowy kwotę stanowiącą równowartość łącznej ceny brutto wskazanej w ofercie Wykonawcy.
2. Zamawiający zastrzega, że wynagrodzenie wykonawcy stanowić będzie iloczyn liczby dostarczonych zgodnie z umową licencji oraz ich ceny jednostkowej wskazanej w ofercie Wykonawcy.
3. Wynagrodzenie za wykonanie przedmiotu umowy płatne będzie na podstawie faktury wystawionej przez Wykonawcę, w terminie 14 dni od daty otrzymania poprawnie wystawionej faktury i dostarczenia przedmiotu umowy Zamawiającemu.

§ 4

Strony wyznaczają do kontaktów związanych z realizacją umowy, w tym do odbioru przedmiotu umowy, następujące osoby:

1) po stronie Zamawiającego – Adam Sieniawski, tel. 58 32 33 133,
   e-mail : adam.sieniawski@arp.gda.pl,
2) po stronie Wykonawcy - ……., tel. ……., e-mail ……

§ 5

1. W przypadku nienależytego wykonania przedmiotu umowy Wykonawca zobowiązuje się do zapłaty Zamawiającemu kary umownej:
   a) za zwłokę w dostawie przedmiotu umowy w wysokości 0,5 % wartości umowy określonej w § 3 ust. 1, za każdy rozpoczęty dzień zwłoki po upływie terminu wskazanego w § 2 ust. 2,
   b) za zwłokę w dostawie przedmiotu opcji w wysokości 2 % wartości niedostarczonego przedmiotu prawa opcji za każdy rozpoczęty dzień zwłoki po upływie terminu wskazanego w § 1 ust. 3,
   c) z tytułu odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy w wysokości 10 % wartości umowy określonej w § 3 ust. 1 niniejszej Umowy.
2. Zamawiającemu przysługuje prawo do odszkodowania uzupełniającego, przekraczającego wysokość kar umownych do wysokości rzeczywiście poniesionej szkody.
3. Wykonawca upoważnia Zamawiającego do potrącania naliczanych kar umownych z faktur wystawionych przez Wykonawcę.

§ 6

1. Wykonawca zobowiązuje się do bezwzględnego zachowania w poufności przez czas nieoznaczony wszelkich informacji i danych uzyskanych od Zamawiającego w związku z realizacją niniejszej umowy i zobowiązuje się nie wykorzystywać tych informacji i danych do jakichkolwiek innych celów bez pisemnej zgody Zamawiającego.
2. Wykonawca zobowiązuje się informować przedstawicieli Zamawiającego o wszystkich zauważonych nieprawidłowościach mogących mieć wpływ na bezpieczeństwo informacji.

§ 7

Agencja Rozwoju Pomorza S.A. oświadcza, że:

1) administratorem danych osobowych jest Agencja Rozwoju Pomorza S.A., Al. Grunwaldzka 472 D, 80 - 309 Gdańsk, NIP 583-000-20-02, Regon 190044530, adres e-mail: sekretariat@arp.gda.pl, tel. +48 58 32 33 101, fax +48 58 32 33 200, zwana dalej Administratorem; Administrator prowadzi operacje przetwarzania Pana danych osobowych;
2) inspektorem ochrony danych osobowych w Agencji Rozwoju Pomorza S.A. jest Lucjan Brudzyński, kontakt: rodo@arp.gda.pl;
3) dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L Nr 119, str. 1);
4) odbiorcami danych osobowych będą osoby lub podmioty, którym udostępniona zostanie umowa w oparciu o przepisy ustawy o dostępie do informacji publicznej; oraz podmioty, z którymi Agencja Rozwoju Pomorza S.A. zawarła stosowne umowy powierzenia związane z przechowywaniem oraz certyfikowanym niszczeniem dokumentów
5) dane osobowe będą przetwarzane w związku z realizacją projektów współfinansowanych ze środków Unii Europejskiej w ramach programów krajowych i międzynarodowych realizowanych przez Agencję Rozwoju Pomorza S.A do upływu terminów wynikających z zawartych umów, jednak nie krócej niż do dnia 31 grudnia 2028 r.,

6) obowiązek podania danych osobowych bezpośrednio dotyczących wykonawcy będącego osobą fizyczną jest niezbędny w celu zawarcia i realizacji umowy;
7) w odniesieniu do danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8) osoba, której dane są przetwarzane, posiada:
   a) na podstawie art. 15 RODO prawo dostępu do danych osobowych jej dotyczących,
   b) na podstawie art. 16 RODO prawo do sprostowania jej danych osobowych (skorzystanie z prawa do sprostowania nie może skutkować zmianą postanowień umowy w zakresie niezgodnym z zapytaniem ofertowym),
   c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (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),
   d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych narusza przepisy RODO;
9) osoba, której dane są przetwarzane, nie posiada:
   a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawa do usunięcia danych osobowych,
   b) na podstawie art. 21 RODO prawa sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. b RODO.

§ 8

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności. W sprawach nieuregulowanych umową zastosowanie mają przepisy kodeksu cywilnego.
2. Strony zgodnie poddają ewentualne spory wynikłe na tle realizacji niniejszej umowy rozstrzygnięciu właściwemu sądowi powszechnemu w Gdańsku.
3. Umowę niniejszą sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.
4. Zamawiający informuje, iż przedmiotowe zamówienie będzie współfinansowane ze środków Unii Europejskiej w ramach programów krajowych i międzynarodowych realizowanych przez Agencję Rozwoju Pomorza S.A., w szczególności:
   a) Europejskiego Funduszu Rozwoju Regionalnego w ramach pomocy technicznej Programu Operacyjnego Inteligentny Rozwój;
   b) Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Pomorskiego na lata 2014 - 2020, projekt pt. „Pomorski Broker Eksportowy. Kompleksowy system wspierania eksportu w województwie pomorskim” oraz projekt pt. „Invest in Pomerania 2020”;
   c) Europejskiego Funduszu Społecznego w ramach Regionalnego Programu Operacyjnego Województwa Pomorskiego na lata 2014 – 2020, projekt pt. „Pomorzanki w Biznesie”;
   d) Funduszu Spójności w ramach Programu Operacyjnego Pomoc Techniczna 2014 – 2020;
   e) Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Europejskiej Współpracy Terytorialnej „Interreg Południowy Bałtyk”, projekt pt. „Circular economy tools to support

innovation in green and blue tourism SMEs (CIRTOINNO)" oraz projekt "Wellbeing Tourism in the South Baltic Region - Guidelines for good practices & Promotion (SBWELL)";

f) Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Europejskiej Współpracy Terytorialnej „Interreg Europa", projekt pt. „Everywhere International SMEs (EIS)";
g) Europejskiego Funduszu Rozwoju Regionalnego w ramach programu Europejskiej Współpracy Terytorialnej „Region Morza Bałtyckiego 2014-2020", projekt pt. „Supporting Non-technological Innovation in Owner-managed Manufacturing SMEs through increased capacity of business intermediaries (SNOwMan)".

Zamawiający **Wykonawca**

Załączniki:

1. Oferta Wykonawcy.
2. Zapytanie ofertowe.