KOMENDA GŁÓWNA POLICJI
02 – 642 Warszawa
ul. Puławska 148/150

REGON: 012137497
NIP: 521 – 31 – 72 - 762

FZ- 8672/15

„ZATWIERDZAM"

ZASTĘPCA DYREKTORA
BIURA FINANSÓW
KOMENDY GŁÓWNEJ POLICJI
Małgorzata KUMICKA
10.11.15

Sprawa nr **252/BŁiI/15/MT**

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA (SIWZ)

Dotyczy: przetargu nieograniczonego poniżej 134.000 Euro, ogłoszonego przez Komendanta Głównego Policji na realizację zamówienia pn.: **Dostawa narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT.**

Warszawa, dnia ..... 2015 r.

Komendant Główny Policji, zwany dalej Zamawiającym, zaprasza do udziału w postępowaniu prowadzonym w trybie przetargu nieograniczonego **na dostawa narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT** zgodnie z wymaganiami określonymi w niniejszej Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej SIWZ.

I. INFORMACJE OGÓLNE:

1. Do udzielenia przedmiotowego zamówienia stosuje się przepisy ustawy z dnia 29 stycznia 2004r. – Prawo zamówień publicznych (t.j. - Dz. U. z 2013 r., poz. 907 z późn zm.), zwanej dalej ustawą Pzp oraz akty wykonawcze wydane na jej podstawie.

2. Do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu o udzielenie zamówienia publicznego stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2014 r. poz. 121), jeżeli przepisy ustawy Pzp nie stanowią inaczej

3. Postępowanie o udzielenie zamówienia publicznego prowadzi się w języku polskim (art. 9 ust. 2 ustawy Pzp). Zamawiający dopuszcza wykorzystanie języka obcego w zakresie określonym w art. 11 ustawy z dnia 7 października 1999r. o języku polskim (Dz. U. z 2011 Nr 43, poz. 224).

II. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO:

KOMENDA GŁÓWNA POLICJI
02-624 Warszawa, ul. Puławska 148/150
Regon: 012137497

Adres do korespondencji:
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH
BIURO FINANSÓW KGP,
02-672 Warszawa, ul. Domaniewska 36/38
tel.22-60120-44,
fax 22-6011857,
e-mail: zamowieniakgp@policja.gov.pl

Informacje związane z przedmiotowym postępowaniem objęte ustawowym wymogiem publikacji na stronie internetowej Zamawiającego będą udostępniane pod adresem: www.policja.pl

III. TRYB UDZIELENIA ZAMÓWIENIA:

1. Postępowanie prowadzone jest w trybie przetargu nieograniczonego, w którym w odpowiedzi na publiczne ogłoszenie o zamówieniu, oferty mogą składać wszyscy zainteresowani Wykonawcy.

2. Zamawiający nie przewiduje przeprowadzenie aukcji elektronicznej, o której mowa w art. 91a ÷ 91c ustawy Pzp.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA:

1. Przedmiotem zamówienia jest dostawa narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT.

   Przedmiot zamówienia został szczegółowo opisany w załączniku nr 1 do SIWZ tj. Opis przedmiotu zamówienia

   CPV – 48821000-9, 30210000-4, 30231000-7

2. Zamawiający nie dopuszcza składanie ofert częściowych.

3. Zamawiający nie dopuszcza składania ofert wariantowych.

4. Zamawiający nie przewiduje możliwości udzielenia zamówienia uzupełniającego o którym mowa w art. 67 ust. 1 pkt. 6 i 7 ustawy Pzp.

5. Zamawiający dopuszcza powierzenie zamówienia podwykonawcom Wykonawcy. W takim wypadku Wykonawca ma obowiązek (zgodnie z art. 36b ust. 1 ustawy Pzp) zawrzeć w ofercie informacje dot. podwykonawstwa. Brak powyższej informacji w ofercie oznaczać będzie, że Wykonawca nie będzie korzystał z podwykonawstwa przy realizacji zamówienia.

6. Zgodnie z art. 29 ustawy Pzp. Zamawiający dopuszcza możliwość składania ofert równoważnych. Ilekroć w niniejszej SIWZ przedmiot zamówienia został określony przez wskazanie znaków towarowych, patentów, pochodzenia itp. intencją Zamawiającego było przedstawienie „typu" towaru spełniającego wymagania Zamawiającego. W związku z tym, dopuszczalne jest zaoferowanie przez Wykonawcę rozwiązania równoważnego, które zagwarantuje nie gorsze normy, parametry i standardy techniczno-jakościowe oraz funkcjonalne. Wykonawca proponując produkty równoważne z opisywanym przez Zamawiającego, zobowiązany jest wykazać, że oferowane przez niego towary spełniają wymagania określone w SIWZ.

7. Ilekroć w dalszych postanowieniach Specyfikacji Istotnych Warunków Zamówienia, mowa jest o przedmiocie zamówienia bez bliższego oznaczenia, należy przez to rozumieć przedmiot zamówienia wskazany w ust. 1.

V. TERMIN WYKONANIA ZAMÓWIENIA:

Termin realizacji zamówienia: **nie później niż do 18.12.2015 r.**

VI. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW:

1. O zamówienie może się ubiegać Wykonawca, który spełnia warunki określone w art. 22 ust. 1 ustawy Pzp, oraz nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 ustawy Pzp.

2. Zamawiający wykluczy z postępowania o udzielenie zamówienia Wykonawcę, który w okresie 3 lat przed wszczęciem postępowania, w sposób zawiniony poważnie naruszył obowiązki zawodowe, w szczególności, gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie. Zamawiający nie wykluczy z postępowania o udzielenie zamówienia Wykonawcy, który udowodni, że podjął konkretne środki techniczne, organizacyjne i kadrowe, które mają zapobiec zawinionemu i poważnemu naruszaniu obowiązków zawodowych w przyszłości oraz naprawił szkody powstałe w wyniku naruszenia obowiązków zawodowych lub zobowiązał się do ich naprawienia.

3. Zamawiający oceni, czy Wykonawca spełnia warunki, o których mowa w ust. 1 na podstawie złożonego wraz z ofertą (zgodnie z art. 44 ustawy Pzp) oświadczenia o spełnieniu warunków udziału w postępowaniu i na podstawie złożonych wraz z ofertą dokumentów żądanych przez Zamawiającego potwierdzających spełnianie tych warunków, o których mowa w rozdziale VII SIWZ.

4. Jeżeli Wykonawca nie wykaże spełniania warunków udziału w postępowaniu, z zastrzeżeniem art. 26 ust. 3 ustawy Pzp, to Zamawiający wykluczy Wykonawcę odpowiednio na podstawie art. 24 ust. 2 pkt. 4 ustawy Pzp.

VII. INFORMACJE O OŚWIADCZENIACH LUB DOKUMENTACH, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY

Zgodnie z przepisami ustawy Pzp oraz Rozporządzenia Prezesa Rady Ministrów z dnia 19 lutego 2013 r. *w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy, oraz form, w jakich te dokumenty mogą być składane* (Dz. U. 2013r. poz. 231.), Wykonawca wraz z ofertą musi złożyć następujące dokumenty:

1. **W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia wykonawcy w okolicznościach o których mowa w art. 24 ust. 1 oraz art. 24b ust 3 ustawy Pzp, w postępowaniach określonych w art. 26 ust. 1 ustawy Pzp, Zamawiający żąda następujących dokumentów:**

1.1. oświadczenia o braku podstaw do wykluczenia;

1.2 aktualnego odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,

1.3 listy podmiotów należących do tej samej grupy kapitałowej albo informację o tym, że nie należy do grupy kapitałowej (wzór stanowi załącznik nr 4 do SIWZ).

2. W celu wykazania potwierdzenia, że oferowany dostawy odpowiadają wymaganiom określonym przez zamawiającego, Wykonawcy składają wraz z ofertą:

2.1 szczegółowy opis oferowanych rozwiązań, potwierdzający wszystkie wymagania określone w załączniku nr 1 do SIWZ wraz z podaniem nazwy, typu, producenta oraz elementów składowych oferowanych urządzeń.

3. Ponadto Wykonawca musi złożyć:
3.1 wypełniony Formularz ofertowy (zalecaną treść formularza zawiera załącznik nr 2 do SIWZ),

4. Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej:
1) zamiast dokumentów wymienionych w pkt 1.2 składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
   - nie otwarto jego likwidacji ani nie ogłoszono upadłości - wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,

5. Wymagana forma składanych dokumentów:
a) dokumenty należy przedstawić w formie oryginałów albo kopii poświadczonych przez Wykonawcę za zgodność z oryginałem,
b) wszelkie czynności Wykonawcy związane ze złożeniem wymaganych dokumentów (w tym m.in.: składanie oświadczeń woli w imieniu Wykonawcy, poświadczanie kserokopii dokumentów za zgodność z oryginałem) muszą być dokonywane przez upoważnionych przedstawicieli Wykonawcy,
c) w przypadku dokonywania czynności związanych ze złożeniem wymaganych dokumentów przez osobę(y) nie wymienioną(e) w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy do oferty należy dołączyć stosowne pełnomocnictwo w formie oryginału lub kopii poświadczonej notarialnie za zgodność z oryginałem,
d) poświadczenie za zgodność z oryginałem winno być sporządzone w sposób umożliwiający identyfikację podpisu,
e) dokumenty sporządzone w języku obcym należy złożyć wraz z ich tłumaczeniem na język polski.

W przypadku nie spełnienia warunków określonych w rozdziale VI Wykonawca zostanie wykluczony z postępowania, a jego oferta zostanie odrzucona zgodnie z art. 89 ust. 1 pkt. 5 ustawy Pzp. O wykluczeniu z postępowania Wykonawca zostanie powiadomiony zgodnie z art. 24 ust. 3 ustawy Pzp, z zastrzeżeniem art. 92 ust. 1 pkt. 3 ustawy Pzp.

VIII. OSOBY UPRAWNIONE DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI ORAZ INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI I PRZEKAZYWANIA OŚWIADCZEŃ ORAZ DOKUMENTÓW:

1. Osobami uprawnionymi przez Zamawiającego do porozumiewania się z Wykonawcami jest w sprawach proceduralnych - Monika Tobar tel. (022) 60 119 82.

2. Zamawiający urzęduje w dni robocze tj. od poniedziałku do piątku w godz. 8.15 - 16.15 (z wyjątkiem dni ustawowo wolnych od pracy).

3. Wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający oraz Wykonawcy przekazywać będą w formie pisemnej, faksem lub drogą elektroniczną z zachowaniem zasad określonych w ustawie Pzp. Zamawiający wymaga aby wszelkie pisma związane z postępowaniem były kierowane na adres do korespondencji określony w rozdziale II niniejszej SIWZ.

4. Korespondencja przesyłana za pomocą faksu po godzinach urzędowania (tj. która wpłynie do Zamawiającego po godzinie 16:15) zostanie zarejestrowana w następnym dniu pracy Zamawiającego.

IX. WYMAGANIA DOTYCZĄCE WADIUM:

1. Przystępując do przetargu, Wykonawca zobowiązany jest wnieść wadium, zaznaczając cel wpłaty, w wysokości 6.000,00 zł (sześć tysięcy złotych).
2. Forma wnoszenia wadium.
   Wadium może być wniesione w jednej lub kilku następujących formach, w:
   - 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. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. Nr 109, poz. 1158 z późn. zm.).
3. Wadium wnoszone w pieniądzu Wykonawca wpłaca przelewem na podany niżej rachunek bankowy Zamawiającego (kserokopię dokumentu potwierdzającego dokonanie powyższej operacji Wykonawca winien dołączyć do oferty):

Komenda Główna Policji Narodowy Bank Polski O/O Warszawa 07 1010 1010 0071 2613 9120 0000 z dopiskiem nr sprawy 252/BŁiI/15/MT

4. Wadium wnosi się przed upływem terminu składania ofert, tj. wadium musi być złożone lub wpłynąć na rachunek Zamawiającego przed upływem terminu składania ofert i musi obejmować cały okres związania ofertą.

5. Wadium wniesione w jednej z form określonych w pkt 2 (z wyłączeniem formy pieniężnej), należy złożyć w formie oryginału w Biurze Finansów KGP przy ul. Domaniewskiej 36/38 w Warszawie pok. 523 (w dniach od poniedziałku do piątku, w godz. 9.00-15.00).
   Nie należy załączać oryginału dokumentu wadialnego do oferty.

6. Dokumenty, o których mowa w pkt 5, muszą być podpisane przez przedstawiciela Gwaranta. Podpis winien być sporządzony w sposób umożliwiający jego identyfikację, np. złożony wraz z imienną pieczątką lub czytelny (z podaniem imienia i nazwiska). Z treści gwarancji winno wynikać bezwarunkowe zobowiązanie Gwaranta do wypłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 46 ust. 4a oraz art. 46 ust. 5 ustawy Prawo zamówień publicznych na każde pisemne żądanie zgłoszone przez Zamawiającego w terminie związania ofertą.

7. Wykonawca, który nie zabezpieczy złożonej oferty wadium w wymaganej formie zostanie wykluczony z postępowania na podstawie art. 24 ust. 2 pkt 2 ustawy Pzp, a jego oferta zostanie uznana za odrzuconą (art. 24 ust. 4 ustawy Pzp).

8. Zamawiający dokona zwrotu wadium lub zatrzyma wadium na zasadach określonych w ustawie Pzp.

9. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 ustawy Pzp, z przyczyn leżących po jego stronie, nie złożył dokumentów lub oświadczeń, o których mowa w art. 25 ust. 1 ustawy Pzp, pełnomocnictw, listy podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy Pzp, lub informacji o tym, że nie należy do grupy kapitałowej, lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3 ustawy Pzp, co powodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej.

X. TERMIN ZWIĄZANIA OFERTĄ:

Termin związania ofertą wynosi 30 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

XI. OPIS SPOSOBU PRZYGOTOWANIA OFERTY:

1. Wykonawca przedstawi ofertę zgodnie z wymaganiami określonymi w niniejszej SIWZ poprzez wypełnienie i podpisanie formularza ofertowego (zalecaną treść formularza stanowi załącznik nr 2 do SIWZ).
2. Wykonawca ma prawo złożyć tylko jedną ofertę we własnym imieniu lub w imieniu innego Wykonawcy (ów).
3. Oferta wraz ze wszystkimi załącznikami - pod rygorem jej odrzucenia - musi być sporządzona w języku polskim (zgodnie z art. 9 ust. 2 ustawy Pzp). Oferta musi być podpisana przez osobę(y) upoważnioną(e) do reprezentowania Wykonawcy wobec osób trzecich.
4. Zgodnie z art. 23 ustawy Pzp Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia (np. w formie konsorcjum) pod warunkiem, że ustanowią oni pełnomocnika określając zgodnie z art. 23 ust. 2 ustawy Pzp zakres jego uprawnień wobec Zamawiającego, a złożona przez nich oferta spełniać będzie następujące wymagania:
   - oferta Wykonawców wspólnie ubiegających się o zamówienie musi być podpisana w taki sposób, aby prawnie zobowiązywała wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia,
   - każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia, musi oddzielnie udokumentować fakt, że nie podlega wykluczeniu z postępowania na podstawie art. 24 ustawy Pzp poprzez złożenie dokumentów określonych w rozdziale VII pkt 1,
   - w odniesieniu do wymogów określonych w art. 22 ust.1 ustawy Pzp Zamawiający będzie brał pod uwagę łączne uprawnienia Wykonawców do wykonywania czynności/działalności wchodzących w zakres zamówienia, ich łączny potencjał techniczny, kadrowy, kwalifikacje, wiedzę i doświadczenie, a także ich łączną sytuację ekonomiczną i finansową, które zostaną potwierdzone poprzez złożenie oświadczenia w pkt. 6 Formularza ofertowego,
   - wszelka korespondencja dokonywana będzie wyłącznie z pełnomocnikiem, wypełniając formularz ofertowy, jak również inne dokumenty powołujące się na Wykonawcę, w miejscu „nazwa i adres Wykonawcy" należy wpisać dane dotyczące pełnomocnika,
   - z treści formularza ofertowego powinno wynikać, że oferta składana jest w imieniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia,
   - w miejsce „pełna nazwa Wykonawcy, adres,..." należy wpisać nazwy Wykonawców i dane umożliwiające ich identyfikację.

5. Oferta i załączniki do oferty (oświadczenia Wykonawcy, zaświadczenia z organów administracji publicznej oraz inne dokumenty) muszą być podpisane przez upoważnionych przedstawicieli Wykonawcy (w sposób zgodny z opisanym w rozdziale VII niniejszej SIWZ - Forma składanych dokumentów).

6. Zamawiający zaleca, by każda strona oferty (wraz z załącznikami do oferty) była ponumerowana kolejnymi numerami, a oferta wraz z załącznikami była zestawiona w sposób uniemożliwiający jej samoistną dekompletację oraz uniemożliwiający zmianę jej zawartości bez widocznych śladów naruszenia.

7. Wszelkie poprawki lub zmiany w treści oferty (w tym w załącznikach do oferty) muszą być parafowane (lub podpisane) własnoręcznie przez osobę(y) upoważnioną(e). Parafka (podpis) winna być naniesiona w sposób umożliwiający identyfikację podpisu (np. wraz z imienną pieczątką osoby sporządzającej parafkę).

8. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty. Wykonawcy zobowiązują się nie podnosić jakichkolwiek roszczeń z tego tytułu względem Zamawiającego.

9. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy Pzp protokół postępowania jest jawny, z zastrzeżeniem art. 8 ust. 3 ustawy Pzp.

10. Zgodnie z art. 8 ust. 3 ustawy Pzp, Wykonawca ma prawo zastrzec informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4. Informacje zawarte w ofercie, stanowiące tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, należy oznaczyć klauzulą: „Dokument stanowi

tajemnicę przedsiębiorstwa w rozumieniu Ustawy o zwalczaniu nieuczciwej konkurencji" i wydzielić w formie załącznika.

XII. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT:

Miejsce i termin składania ofert:

1. Ofertę wraz ze wszystkimi wymaganymi oświadczeniami lub dokumentami, należy umieścić w zamkniętej kopercie, zapieczętowanej w sposób gwarantujący zachowanie poufności jej treści oraz zabezpieczającej jej nienaruszalność do terminu otwarcia ofert.
   Koperta powinna opisana według poniższego wzoru:

Komenda Główna Policji, Biuro Finansów ul. Domaniewska 36/38, 02-672 Warszawa Przetarg nr 252/BŁiI/15/MT **Oferta na dostawę narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT.** Nie otwierać przed ..18..11....2015 r.

UWAGA
Przesyłka zawierająca ofertę, przekazywana za pośrednictwem poczty kurierskiej musi być oznakowana (opisana) zewnętrznie w sposób określony powyżej.

2. Koperta poza oznakowaniem jak wyżej powinna być opatrzona dokładną nazwą i adresem Wykonawcy.

3. Ofertę należy złożyć do dnia ..18..11....**2015 r. do godz. 10.30 w** Biurze Finansów KGP, 02-672 Warszawa, ul. Domaniewska 36/38, pokój 435, tel. 0-22-6013204, w godz. 8.30 – 15.30 (od poniedziałku do piątku).

4. Wykonawca (na żądanie) otrzyma pisemne potwierdzenie złożenia oferty.

5. Konsekwencje złożenia oferty niezgodnie z ww. opisem (np. potraktowanie oferty jako zwykłej korespondencji i nie dostarczenie jej na miejsce składania ofert w terminie określonym w SIWZ) ponosi Wykonawca.

6. Oferta złożona po terminie zostanie zwrócona Wykonawcy bez otwierania po upływie terminu przewidzianego na wniesienie odwołania.

7. Publiczna sesja otwarcia ofert odbędzie się w siedzibie Zamawiającego w Warszawie przy ul. Domaniewskiej 36/38, w dniu ...18..11.....**2015 r. o godz. 11.00.**

Zmiana i wycofanie oferty:

1. Wykonawca może wprowadzić zmianę do treści złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmiany przed terminem składania ofert. Zmiana do oferty musi być dokonana według zasad obowiązujących przy składaniu oferty, tj. musi być złożona w zamkniętej kopercie odpowiednio oznakowanej z dopiskiem „ZMIANA".

2. Koperty oznakowane dopiskiem „ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany. Po stwierdzeniu poprawności procedury dokonania zmiany zawartość koperty zostanie dołączona do oferty.

3. Wykonawca ma prawo wycofać ofertę pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie (oświadczenie) o wycofaniu oferty przed terminem składania ofert.

UWAGA:
Do składanego oświadczenia (zmiana lub wycofanie oferty) należy dołączyć stosowny dokument potwierdzający prawo osoby podpisującej oświadczenie do występowania w imieniu Wykonawcy.

XIII. OPIS SPOSOBU OBLICZENIA CENY OFERTOWEJ ORAZ INFORMACJA O WALUCIE W JAKIEJ BĘDĄ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ:

1. Przez cenę ofertową należy rozumieć cenę w rozumieniu art. 3 ust. 1 pkt 1 ustawy z dnia 9 maja 2014 r. o informowania o cenach towarów i usług (Dz. U. 2014 poz. 915)

2. Cena ofertowa musi obejmować wszelkie koszty związane z realizacją umowy m.in. opłaty i podatki, opłaty celne, szkolenia, koszty opakowania oraz ewentualne upusty i rabaty, a także koszty dostarczenia (transportu) przedmiotu umowy do miejsca wyznaczonego przez Zamawiającego.

3. W przypadku różnicy pomiędzy ceną ofertową brutto określoną przez Wykonawcę słownie i liczbą np. w formularzu ofertowym Zamawiający przyjmie jako prawidłową wartość oferty określoną słownie.

4. Jeżeli w postępowaniu zostanie złożona oferta, której wybór prowadziłby do powstania obowiązku podatkowego Zamawiającego na podstawie przepisów o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek odprowadzić zgodnie z obowiązującymi 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.

5. Rozliczenia pomiędzy Zamawiającym a Wykonawcą dokonywane będą w złotych polskich.

XIV. OPIS KRYTERIÓW Z PODANIEM ICH ZNACZENIA I SPOSOBU OCENY OFERT:

1. Oceniane kryteria i ich znaczenie:

Lp.	Nazwa kryterium	Ranga w %	Sposób oceny
1.	Cena oferty brutto (C)	86%	Minimalizacja
2.	Okres gwarancji (G)	14%	Maksymalizacja

2. Ocena ofert odbędzie się zgodnie z poniższymi wzorami.

a) Sposób obliczenia punktów w odniesieniu do kryterium „Cena oferty brutto"

C - waga 86% (maksymalnie Wykonawca może otrzymać 86 punktów)

$$C = \frac{\textbf{najniższa cena oferty brutto z przedłożonych ofert}}{\textbf{cena oferty brutto oferty badanej}} \times 86$$

b) Sposób obliczenia punktów w odniesieniu do kryterium „Okres gwarancji"

G - waga 14 % (maksymalnie Wykonawca może otrzymać 14 punktów)

G – 1 pkt. za każde dodatkowe 6 miesięcy gwarancji w stosunku do minimalnego okresu gwarancji określonego przez Zamawiającego.

Uwaga:
1) Przedłużenie gwarancji ponad wymagania minimalne musi być podane w pełnych 6 miesiącach. W przypadku podania w niepełnym 6 miesiącach Zamawiający dokonana zaokrąglenia w „dół" odpowiednio do pełnych 6 miesięcy.
2) W ramach kryterium „Okres gwarancji" Wykonawca może uzyskać maksymalnie 14 punktów, z czego na przedłużenie okresu gwarancji na:
- serwer– wykonawca może uzyskać maksymalnie – 2 pkt.
- terminal – wykonawca może uzyskać maksymalnie – 2 pkt.
- monitor 28''- wykonawca może uzyskać maksymalnie – 2 pkt.
- stanowiska administracyjne – wykonawca może uzyskać maksymalnie – 2 pkt.
- stanowiska do prezentacji – wykonawca może uzyskać maksymalnie – 2 pkt.
- monitor 50'' – wykonawca może uzyskać maksymalnie – 2 pkt.
- mobilne stanowiska typ A i typ B - wykonawca może uzyskać maksymalnie – 2 pkt.
3) W przypadku wpisania cyfry 0 (lub brak wpisu) Zamawiający uzna, że Wykonawca nie przedłuża terminu okresu gwarancji oraz oferuje minimalne okresy gwarancji określone odpowiednio w załączniku nr 3 do umowy.

c) Łączna ilość punktów zostanie obliczona zgodnie z poniższym wzorem:

Łp= C+G

3. Zasady wyboru oferty i udzielenia zamówienia:

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie Pzp i niniejszej SIWZ oraz uzyska najwyższą liczbę punktów obliczoną według wzoru określonego w pkt. c).

XV. INFORMACJE DOTYCZĄCE WYBORU NAJKORZYSTNIEJSZEJ OFERTY Z ZASTOSOWANIEM AUKCJI ELEKTRONICZNEJ:

1. Zamawiający nie przewiduje dokonanie wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej, na zasadach określonych w art. 91a-91c ustawy Pzp.

XVI. INFORMACJA O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO:

1. Zamawiający po dokonaniu wyboru najkorzystniejszej oferty zawiadomi pisemnie o wynikach postępowania wszystkich Wykonawców, którzy złożyli oferty.

2. Zamawiający poinformuje Wykonawcę, którego oferta została uznana za najkorzystniejszą, o terminie i miejscu zawarcia umowy.

3. W przypadku, gdy za najkorzystniejszą zostanie uznana oferta Wykonawcy prowadzącego działalność w formie spółki z ograniczoną odpowiedzialnością, a wartość złożonej przez niego oferty przekroczy dwukrotność kapitału zakładowego spółki, wówczas przed podpisaniem umowy Wykonawca ten przedłoży dokument wymagany treścią art. 230 ustawy z dnia 15 września 2000 r. – Kodeks spółek handlowych (Dz. U. 2013 poz. 1030 z późn. zm.), chyba, że ww. dokument został złożony przez Wykonawcę w ofercie.

4. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, których oferta została uznana za najkorzystniejszą, w wypadku dołączenia do oferty pełnomocnictwa (o którym mowa w art. 23 ust. 2 ustawy Pzp) tylko do reprezentowania ich w postępowaniu o udzielenie zamówienia publicznego, przedłożą stosowne pełnomocnictwo do podpisania umowy w sprawie zamówienia publicznego. Ponadto, przed podpisaniem umowy, Zamawiający wymagać będzie przedłożenia umowy regulującej współpracę Wykonawców występujących wspólnie.

5. Przed podpisaniem umowy Wykonawca dostarczy Zamawiającemu specyfikację ilościową-cenową, która będzie stanowić załącznik do umowy.

XVII. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY:

1. Przed podpisaniem umowy Zamawiający będzie wymagał od Wykonawcy, którego oferta została wybrana, wniesienia zabezpieczenia należytego wykonania umowy w wysokości 10 % ceny całkowitej podanej w ofercie.

2. Forma wnoszenia zabezpieczenia należytego wykonania umowy.
Zabezpieczenie może być wnoszone w następujących formach:
   - w pieniądzu,
   - w poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   - w gwarancjach bankowych,
   - w gwarancjach ubezpieczeniowych,
   - poręczeniach udzielanych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. 2014 r. poz. 1804 z późn. zm.).

Gwarancja musi być podpisana przez przedstawiciela Gwaranta. Podpis winien być sporządzony w sposób umożliwiający jego identyfikację, np. złożony wraz z imienną pieczątką lub czytelny (z podaniem imienia i nazwiska). Z treści gwarancji (bankowej, ubezpieczeniowej) winno wynikać bezwarunkowe zobowiązanie Gwaranta do wypłaty Zamawiającemu kwoty zabezpieczenia należytego wykonania umowy na każde pisemne żądanie zgłoszone przez Zamawiającego.
Szczegóły dotyczące wniesienia zabezpieczenia należytego wykonania umowy zostaną podane Wykonawcy, którego oferta została uznana za najkorzystniejszą po rozstrzygnięciu postępowania o udzielenie zamówienia publicznego wraz z zastosowaniem art. 150, ust. 3-6 ustawy Pzp.

3. Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy w sposób określony w projekcie umowy – załącznik nr 5 do SIWZ.

XVIII. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWARTEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO LUB PROJEKT UMOWY:

1. Zamawiający podpisze z wybranym Wykonawcą umowę zgodnie z załączonym do SIWZ projektem umowy (załącznik nr 5).

XIX. WARUNKI DOKONANIA ZMIAN POSTANOWIEŃ ZAWARTEJ UMOWY

1. Strony przewidują możliwość dokonywania zmian w treści umowy w stosunku do treści oferty Wykonawcy w sytuacjach określony w projekcie umowy (załącznik nr 5).

XX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO:

1. Wykonawcom przysługują środki ochrony prawnej określone w Dziale VI ustawy Pzp.

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

3. Odwołanie wnosi się w terminie 5 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane w sposób określony w art. 27 ust. 2 ustawy Pzp. albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób.

4. Odwołanie wobec treści ogłoszenia o zamówieniu oraz wobec postanowień SIWZ wnosi się w terminie 5

dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub SIWZ na stronie internetowej.

5. Odwołanie wobec czynności innych niż określone w pkt. 3 i 4 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.

6. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo elektronicznej opatrzonej bezpiecznym podpisem elektronicznym weryfikowanych za pomocą ważnego kwalifikowanego certyfikatu.

Załączniki do specyfikacji istotnych warunków zamówienia, stanowiące jej integralną część:
Załącznik nr 1 – Opis przedmiotu zamówienia
Załącznik nr 2 – Formularz ofertowy,
Załącznik nr 3 - Oświadczenie o braku podstaw do wykluczenia,
Załącznik nr 4 – Informacja o której mowa w art. 26 ust. 2d ustawy Pzp.,
Załącznik nr 5 – Projekt umowy,

Załącznik nr 1 do SIWZ
nr sprawy 252/BŁiI/15/MT

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest:

„Zakup narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT" :

1. **Zakup serwera – szt. 1 w ukompletowaniu:**

   lub równoważny spełniających warunki wyposażenia:

   - Procesor CPU: minimum szt. 1, charakteryzujący się posiadaniem min 6 rdzeni fizycznych o częstotliwości taktowania co najmniej 1.9 GHz, wykonanego w technologii x86 64 bit, pamięci podręcznej L3 min 15MB, wyposażony w wirtualizację sprzętową typ. Instrukcja VT-x lub podobna, który w testach CPU Benchmarks osiąga średni wynik powyżej 5918 pkt. (źródło www.cpubenchmark.net) przykładowym procesorem spełniającym w/w kryteria jest Intel Xeon E5-2609 v3,
   - Pamięć RAM: min. 8 GB DDR4
   - Dysk HDD: 4 x LFF SATA 1TB lub większy,
   - Kontroler: SATA B140i
   - Interfejs sieciowy Ethernet 1Gbit/s,
   - Obudowa: typu Rack 1U
   - Zasilacz: 2 x 550W
   - Karta zarządzająca: typu ILO zgodna z posiadanym przez Zamawiającego systemem HP SIM.

2. **Zakup stanowisk terminalowych do posiadanego przez Zamawiającego środowiska wirtualizacji desktopów firmy VMware - szt. 7 (zestawów) w ukompletowaniu:**

   a) Terminal HP T310 Zero Client

   lub równoważny spełniających warunki wyposażenia:

   - Procesor CPU wspierający technologię PCoIP,
   - Pamięć RAM: min. 512 MB SDRAM DDR3
   - Pamięć Flash: min. 256B,
   - Protokoły: VMware Horizon View through PCoIP,

- Interfejs sieciowy: 10/100/1000 Gigabit Ethernet (WOL),
- Porty: 4 x USB 2.0, 1xRJ45, 1x GN mikrofonowe, 1x GN Słuchawkowe, 1x DVI-D, 1xDVI-I
- Wsparcie obsługi do 2 wyświetlaczy: 1 port DVI-D, 1 port DVI-I o rozdzielczości max. 1920x1200 przy 60Hz lub pojedynczy wyświetlacz cyfrowy o rozdzielczości do 2560x1600 z użyciem niestandardowego przewodu DVI dual-link,
- Mysz,
- Klawiatura
- Rozszerzona usługa gwarancyjna 36 miesięcy

b) Monitor LED 28"

spełniających warunki wyposażenia:

- Matryca TFT IPS 28" lub większa,
- Obsługa rozdzielczości min. 3840 x 2160 pix,
- Parametry wyświetlania od 300 cd/m2,
- Kontrast 1000:1 lub wyższy,
- Kąt widzenia poziomy i pionowy od 170 stopni lub wyższy,
- Regulacja cyfrowa,
- Wbudowane głośniki,
- Dodatkowe złącza: MHL-HDMI, Mini Display Port, Display Port.

3. **Zakup stanowisk administracyjnych do zarządzania posiadanym przez Zamawiającego oprogramowaniem firmy Check Point i VMware oraz wirtualizacji środowisk sieciowych i desktopowych – szt. 6 (zestawów) w ukompletowaniu:**

a) Jednostka centralna:

spełniająca warunki wyposażenia:

- Procesor: CPU charakteryzujący się posiadaniem min 4 rdzeni fizycznych z możliwością obsługi co najmniej dwóch wątków przez każdy rdzeń, o częstotliwości taktowania co najmniej 4.0 GHz, wykonanego w technologii x86 64 bit, pamięci podręcznej L3 min 8MB, wyposażony w wirtualizację sprzętową typ. Instrukcja VT-x lub podobna, który w testach CPU Benchmarks osiąga średni wynik powyżej 10100 pkt. (źródło www.cpubenchmark.net) przykładowym procesorem spełniającym w/w kryteria jest Intel Core i7 4790K),
- Pamięć RAM: 32 GB (z możliwością rozbudowy),

- Dysk HDD: min. 1TB lub większy,
- Karta graficzna: min Open GL 4.0, DirectX 11.1, OpenCL 1.2, HDMI, DVI-D (zgodna z NVIDIA Quadro K2200) lub lepsza. . Ilość i konfiguracja interfejsów karty musi umożliwiać podłączenia co najmniej dwóch monitorów jednocześnie, w różnych konfiguracjach,
- Porty USB: min 2 porty USB3.0,
- Napęd optyczny: DVD-WR,
- Interfejs sieciowy Ethernet 1Gbit/s,
- Mysz, Klawiatura: nożycowa membranowa lub mechaniczna
- System Operacyjny: Microsoft Windows 8.1 PL Professional 64 bit lub wyższy lub równoważny w zakresie:

1. obsługi, pełnej zgodności i kompatybilności dla posiadanych przez Zamawiającego aplikacji (VMware vSphere Client 5.5 Update 3, VMware vCenter Conventer Standalone Client, Check Point SmartConsole NGSE i R77.30, Check Point Endpoint Security, Check Point Identity Agent, LDAP Admin Tool Profesional 6.2, IBM Lotus Domino Console, NetApp OnCommand System Manager 3.1.2, Secure CRT 6.0, RSA Control Center, Synology Cloud Station). Dostarczone oprogramowanie powinno spełniać wymagania gwarancyjne i serwisowe oraz umożliwiać wykupienie usługi wsparcia technicznego dla w/w aplikacji,
2. dostępności dwóch rodzajów graficznego interfejsu użytkownika:

a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
b) dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych.,

3. interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim,
4. zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe,
5. wbudowany system pomocy w języku polskim,
6. graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
7. funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego,
8. funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika,
9. możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne,
10. możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
11. dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
12. wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6,
13. wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,

14. wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
15. funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
16. możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
17. rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
18. możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
19. zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników,
20. mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu,
21. zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
22. zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi,
23. możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących),
24. wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny,
25. automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
26. mechanizmy logowania do domeny w oparciu o:

a) login i hasło,
b) karty z certyfikatami (smartcard),
c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

27. mechanizmy wieloelementowego uwierzytelniania,
28. wsparcie dla uwierzytelniania na bazie Kerberos v. 5,
29. wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
30. wsparcie dla algorytmów Suite B (RFC 4869),
31. wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
32. wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk,
33. wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,
34. wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
35. zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,

36. rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
37. rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
38. transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
39. zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe,
40. udostępnianie modemu,
41. oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
42. możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
43. identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
44. możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy 4 użyciu numerów identyfikacyjnych sprzętu),
45. wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
46. mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika.,
47. wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB,
48. wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych,
49. możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych,
50. możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.

- Oprogramowanie do wirtualizacji: VMware Workstation 12 Pro
  lub równoważne w zakresie obsługi, pełnej zgodności i kompatybilności z posiadanym przez Zamawiającego środowiskiem VMware vSphere 4.1, 6.0, VMware vCenter Server 5 Standard for View, VMware vSphere 5 Desktop, VMware View Enterprise. Dostarczone oprogramowanie powinno spełniać wymagania gwarancyjne i serwisowe w zakresie współpracy z w/w oprogramowaniem oraz powinno umożliwiać wykupienie usługi wsparcia technicznego.

- Obudowa: typu Tower

b) Monitor LED 28":

spełniający warunki wyposażenia:

- Matryca TFT IPS 28" lub większa,
- Obsługa rozdzielczości min. 3840 x 2160 pix,
- Parametry wyświetlania od 300 cd/m2,
- Kontrast 1000:1 lub wyższy,
- Kąt widzenia poziomy i pionowy od 170 stopni lub wyższy,
- Regulacja cyfrowa,
- Wbudowane głośniki,
- Dodatkowe złącza: MHL-HDMI, Mini Display Port, Display Port.

4. **Zakup stanowisk do prezentacji / analizy zdarzeń – szt. 2 (zestawów) w ukompletowaniu:**

a) Jednostka centralna:

spełniająca warunki wyposażenia:

- Procesor: CPU charakteryzujący się posiadaniem min 4 rdzeni fizycznych z możliwością obsługi co najmniej dwóch wątków przez każdy rdzeń, o częstotliwości taktowania co najmniej 4.0 GHz, wykonanego w technologii x86 64 bit, pamięci podręcznej L3 min 8MB, wyposażony w wirtualizację sprzętową typ. Instrukcja VT-x lub podobna, który w testach CPU Benchmarks osiąga średni wynik powyżej 10100 pkt. (źródło www.cpubenchmark.net) przykładowym procesorem spełniającym w/w kryteria jest Intel Core i7 4790K),
- Pamięć RAM: 32 GB (z możliwością rozbudowy),
- Dysk HDD: min. 1TB lub większy,
- Karta graficzna: min Open GL 4.0, DirectX 11.1, OpenCL 1.2, HDMI, DVI-D (zgodna z NVIDIA Quadro K2200) lub lepsza. . Ilość i konfiguracja interfejsów karty musi umożliwiać podłączenia co najmniej dwóch monitorów jednocześnie, w różnych konfiguracjach,
- Porty USB: min 2 porty USB3.0,
- Napęd optyczny: DVD-WR,
- Interfejs sieciowy Ethernet 1Gbit/s,
- Mysz, Klawiatura: nożycowa membranowa lub mechaniczna
- System Operacyjny: Microsoft Windows 8.1 PL Professional 64 bit lub wyższy lub równoważny zgodnie z opisem określonym w pkt. 3
- Obudowa: typu Tower

b) Monitor LED 50" – szt. 2 (na jednostkę) w ukompletowaniu:

spełniający warunki wyposażenia:

- Matryca LED 50" lub większa,
- Obsługa technologii 4K,

- Obsługa rozdzielczości min. 3840 x 2160 pix,
- System montażu do ściany VESA,
- Uchwyt ścienny uchylny VESA z wyposażeniem,
- Złącza: HMDI, DVI-D w technologii 4K

Dodatkowe złącza: MHL-HDMI, Mini Display Port, Display Port.

5. **Zakup mobilnych stanowisk administracyjnych typu A – szt. 3 w ukompletowaniu:**
   - Procesor: CPU charakteryzujący się posiadaniem min 4 rdzeni fizycznych z możliwością obsługi co najmniej dwóch wątków przez każdy rdzeń, o częstotliwości taktowania co najmniej 2,8 GHz. Wykonanego w technologii x86 64 bit, pamięci podręcznej L3 min 6 MB, wyposażony w wirtualizację sprzętową typ. Instrukcja VT-x lub podobna, który w testach CPU Benchmarks osiąga średni wynik powyżej 10100 pkt. (źródło www.cpubenchmark.net), przykładowym procesorem spełniającym w/w kryteria jest Intel Core i7 4980HQ @ 2.80 GHz),
   - Pamięć RAM: min. 16 GB,
   - Wyświetlacz: z podświetlaniem LED w technologii IPS, przekątna ekranu min. 15,4", rozdzielczość min. 2880 x 1800 pix, min. 220 pix na cal (ppi)
   - Dysk HDD w technologii SSD o rozmiarze min. 1 TB,
   - Interfejs sieciowy Ethernet 1Gbit/s (RJ45),
   - System Operacyjny: Mac OS X Yosemite lub równoważny w zakresie obsługi, pełnej zgodności i kompatybilności dla posiadanego przez Zamawiającego oprogramowania firmy Check Point Endpoint Security z modułem Media Encryption Offline Access Tool.
   - Dodatkowy zasilacz zgodny z interfejsem MagSafe 2,
   - Oprogramowanie biurowe: Microsoft Office 2011 (Mac) lub równoważne w języku polskim, zawierające edytor tekstu, arkusz kalkulacyjny, program do tworzenia prezentacji, program pocztowy. Pakiet komercyjny, przeznaczony dla klientów indywidualnych, instytucjonalnych i biznesowych, oraz użytkowników domowych i małych firm.

     Wymagania odnośnie interfejsu użytkownika:
     1. pełna polska wersja językowa interfejsu użytkownika,
     2. prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych,
     3. możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową Active Directory.

     Pakiet zintegrowanych aplikacji biurowych musi zawierać:
     1. edytor tekstów,
     2. arkusz kalkulacyjny,
     3. narzędzie do przygotowywania i prowadzenia prezentacji,
     4. narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami).

Edytor tekstów musi umożliwiać:

1. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
2. wstawianie oraz formatowanie tabel,
3. wstawianie oraz formatowanie obiektów graficznych,
4. wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne),
5. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
6. automatyczne tworzenie spisów treści,
7. formatowanie nagłówków i stopek stron,
8. sprawdzanie pisowni w języku polskim,
9. śledzenie zmian wprowadzonych przez użytkowników,
10. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
11. określenie układu strony (pionowa/pozioma),
12. wydruk dokumentów,
13. wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną,
14. pracę na dokumentach utworzonych przy pomocy Microsoft Word 2003 lub Microsoft Word 2007 i 2010 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu,
15. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji,
16. wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze bazujące na schematach XML z Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, które po wypełnieniu umożliwiają zapisanie pliku XML w zgodzie z obowiązującym prawem,
17. wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi (kontrolki) umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa,
18. wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska udostępniającego formularze i pozwalające zapisać plik wynikowy w zgodzie z Rozporządzeniem o Aktach Normatywnych i Prawnych.

Arkusz kalkulacyjny musi umożliwiać:

1. tworzenie raportów tabelarycznych,
2. tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
3. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
4. tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice),
5. tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych,
6. wyszukiwanie i zamianę danych,
7. wykonywanie analiz danych przy użyciu formatowania warunkowego,
8. nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
9. nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności,
10. formatowanie czasu, daty i wartości finansowych z polskim formatem,
11. zapis wielu arkuszy kalkulacyjnych w jednym pliku.
12. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2003 oraz Microsoft Excel 2007 i 2010, z

uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
13. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji

Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
1. przygotowywanie prezentacji multimedialnych, które będą prezentowanie przy użyciu projektora multimedialnego,
2. drukowanie w formacie umożliwiającym robienie notatek,
3. napisanie jako prezentacja tylko do odczytu,
4. nagrywanie narracji i dołączanie jej do prezentacji,
5. opatrywanie slajdów notatkami dla prezentera,
6. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
7. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
8. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
9. możliwość tworzenia animacji obiektów i całych slajdów,
10. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
11. pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2003, MS PowerPoint 2007 i 2010.

Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
1. obieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
2. filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
3. tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
4. automatyczne grupowanie poczty o tym samym tytule,
5. tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
6. oflagowanie poczty elektronicznej z określeniem terminu przypomnienia,
7. zarządzanie kalendarzem,
8. udostępnianie kalendarza innym użytkownikom,
9. przeglądanie kalendarza innych użytkowników,
10. zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
11. zarządzanie listą zadań,
12. zlecanie zadań innym użytkownikom,
13. zarządzanie listą kontaktów,
14. udostępnianie listy kontaktów innym użytkownikom,
15. przeglądanie listy kontaktów innych użytkowników,
16. możliwość przesyłania kontaktów innym użytkowników,
17. oprogramowanie winno być dostarczone z bezterminową licencją na użytkowanie.

- Oprogramowanie do wirtualizacji: VMware Fusion 8 Pro
lub równoważne w zakresie obsługi, pełnej zgodności i kompatybilności z posiadanym przez Zamawiającego środowiskiem VMware vSphere 4.1, 6.0, VMware vCenter Server 5 Standard for View, VMware vSphere 5 Desktop, VMware View Enterprise. Dostarczone oprogramowanie powinno spełniać wymagania gwarancyjne i serwisowe w zakresie współpracy z w/w oprogramowaniem oraz powinno umożliwiać wykupienie usługi wsparcia technicznego.

- Oprogramowanie antywirusowe z modułem zapory (Firewall): ESET ENDPOINT SECURITY for Mac OS X z licencją na okres 3 lat lub równoważne w zakresie:

Wymagania ogólne:
1. pełne wsparcie dla systemu Mac OS X Yosemite,
2. wersja programu dla stacji roboczych Windows w języku polskim,
3. pomoc w programie i dokumentacja do programu dostępna w języku polskim,
4. skuteczność programu potwierdzona nagrodami VB100 i co najmniej dwie inne niezależne organizacje takie jak ICSA labs lub Check Mark.

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. skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików,
5. możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu,
6. 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,
7. możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania),
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. możliwość skanowania dysków sieciowych i dysków przenośnych,
11. skanowanie plików spakowanych i skompresowanych,
12. możliwość definiowania listy rozszerzeń plików, które mają być skanowane (w tym z uwzględnieniem plików bez rozszerzeń),
13. możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach,
14. możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu,
15. brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu,
16. użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera,
17. w momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji,
18. ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera,
19. 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,
20. wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego),
21. skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Mozilla Thunderbird do wersji 5.x i Windows Live Mail,
22. 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),

23. automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji,
24. możliwość definiowania różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie,
25. możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail,
26. skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie,
27. 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,
28. możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora,
29. automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji,
30. możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie,
31. program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS,
32. program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe,
33. administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego,
34. aplikacja musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika,
35. procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym,
36. użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego,
37. w przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne,
38. 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,
39. możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika,
40. do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika,
41. możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia,
42. dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe,
43. możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta,
44. możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła,
45. 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,

46. hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji musi być takie samo,
47. system antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku,
48. system antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym,
49. 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 oraz urządzeń przenośnych,
50. funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model,
51. 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,
52. aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika,
53. w momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika,
54. użytkownik ma posiadać możliwość takiej konfiguracji aplikacji aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika,
55. program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS),
56. moduł HIPS musi posiadać możliwość pracy w jednym z czterech trybów:
    - tryb automatyczny z regułami gdzie aplikacja automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    - tryb interaktywny, w którym to aplikacja pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    - tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    - tryb uczenia się, w którym aplikacja uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu aplikacja musi samoczynnie przełączyć się w tryb pracy oparty na regułach.
57. tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego,
58. użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól,
59. 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,
60. 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,
61. 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,
62. automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu,
63. możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami,
64. aplikacja musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji,

65. aplikacja musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http,
66. aplikacja musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback),
67. program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa),
68. aplikacja musi być w pełni zgodna z technologią Network Access Protection (NAP),
69. program ma być w pełni zgodny z technologią CISCO Network Access Control,
70. aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym,
71. w momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji,
72. użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie aplikacja włączała powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie,
73. program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania,
74. wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu,
75. w trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór następujących modułów do instalacji: ochrona antywirusowa i antyspywerowa, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, kopia dystrybucyjna, Obsługa technologii Microsoft NAP.

Ochrona przed spamem:

1. ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird wykorzystująca filtry Bayes-a, białą i czarną listę oraz bazę charakterystyk wiadomości spamowych,
2. program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej,
3. pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail, Windows Live Mail oraz Mozilla Thunderbird – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego,
4. automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego,
5. możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym,
6. możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam,
7. możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam,
8. program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci" obecnym w programie Microsoft Outlook,
9. program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana" oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana",
10. program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall):

1. zapora osobista ma pracować jednym z 5 trybów:
    - tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące,
    - tryb automatyczny z wyjątkami - działa podobnie jak tryb automatyczny, ale umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
    - tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo),
    - tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany,
    - tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji.
2. możliwość tworzenia list sieci zaufanych,
3. możliwość dezaktywacji funkcji zapory sieciowej na kilka sposobów: pełna dezaktywacja wszystkich funkcji analizy ruchu sieciowego, tylko skanowanie chronionych protokołów oraz dezaktywacja do czasu ponownego uruchomienia komputera,
4. możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego,
5. możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję,
6. możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń,
7. możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu,
8. możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet,
9. wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych,
10. wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu,
11. program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6,
12. możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci,
13. administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci,
14. profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora,
15. 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, aktywności wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych konkretny interfejs sieciowy w systemie,
16. podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6,
17. opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci,
18. możliwość aktualizacji sterowników zapory osobistej po restarcie komputera.

Kontrola dostępu do stron internetowych:

1. aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych,
2. moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły,

3. dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego,
4. profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika,
5. aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii,
6. podstawowe kategorie w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii,
7. lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta,
8. użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.

Konsola administracyjna – zakres funkcjonalny:
1. centralna instalacja programów służących do ochrony stacji roboczych Windows,
2. centralne zarządzanie programami służącymi do ochrony stacji roboczych Windows/ Linux/ MAC OS,
3. centralna instalacja oprogramowania na końcówkach (stacjach roboczych) z systemami operacyjnymi typu 2000/XP Professional/Vista/Windows7/Windows 8,
4. do instalacji centralnej i zarządzania centralnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy,
5. komunikacja miedzy serwerem a klientami może być zabezpieczona hasłem,
6. centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci,
7. kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup,
8. możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej,
9. możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych),
10. możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy,
11. możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu,
12. możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych,
13. możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów,
14. możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci,
15. możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne),
16. możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na stacjach Windows Microsoft Windows 8 / 7 / Vista / XP / 2000, Windows Server 2000, 2003, 2008, 2008 R2, 2012, SBS 2003, 2003 R2, 2008, 2011,
17. możliwość rozdzielenia serwera centralnej administracji od konsoli zarządzającej, w taki sposób, że serwer centralnej administracji jest instalowany na jednym serwerze/ stacji a

konsola zarządzająca na tym samym serwerze i na stacjach roboczych należących do administratorów,

18. możliwość wymuszenia konieczności uwierzytelniania stacji roboczych przed połączeniem się z serwerem zarządzającym. Uwierzytelnianie przy pomocy zdefiniowanego na serwerze hasła,
19. do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie żadnych dodatkowych baz typu MSDE lub MS SQL. Serwer centralnej administracji musi mieć własną wbudowaną bazę w pełni kompatybilną z formatem bazy danych programu Microsoft Access,
20. serwer centralnej administracji ma oferować administratorowi możliwość współpracy przynajmniej z trzema zewnętrznymi motorami baz danych w tym minimum z: Microsoft SQL Server, MySQL Server oraz Oracle,
21. do instalacji serwera centralnej administracji nie jest wymagane zainstalowanie dodatkowych aplikacji takich jak Internet Information Service (IIS) czy Apache,
22. możliwość ręcznego (na żądanie) i automatycznego generowania raportów (według ustalonego harmonogramu) w formacie HTML lub CSV,
23. aplikacja musi posiadać funkcjonalność, która umożliwi przesłanie wygenerowanych raportów na wskazany adres email,
24. do wysłania raportów aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na stacji gdzie jest uruchomiona usługa serwera,
25. możliwość tworzenia hierarchicznej struktury serwerów zarządzających i replikowania informacji pomiędzy nimi w taki sposób, aby nadrzędny serwer miał wgląd w swoje stacje robocze i we wszystkie stacje robocze serwerów podrzędnych (struktura drzewiasta),
26. serwer centralnej administracji ma oferować funkcjonalność synchronizacji grup komputerów z drzewem Active Directory. Po synchronizacji automatycznie są umieszczane komputery należące do zadanych grup w AD do odpowiadających im grup w programie. Funkcjonalność ta nie może wymagać instalacji serwera centralnej administracji na komputerze pełniącym funkcję kontrolera domeny,
27. serwer centralnej administracji ma umożliwiać definiowanie różnych kryteriów wobec podłączonych do niego klientów (w tym minimum przynależność do grupy roboczej, przynależność do domeny, adres IP, adres sieci/podsieci, zakres adresów IP, nazwa hosta, przynależność do grupy, brak przynależności do grupy). Po spełnieniu zadanego kryterium lub kilku z nich stacja ma otrzymać odpowiednią konfigurację,
28. serwer centralnej administracji ma być wyposażony w mechanizm informowania administratora o wykryciu nieprawidłowości w funkcjonowaniu oprogramowania zainstalowanego na klientach w tym przynajmniej informowaniu o: wygaśnięciu licencji na oprogramowanie, o tym że zdefiniowany procent z pośród wszystkich stacji podłączonych do serwera ma nieaktywną ochronę, oraz że niektórzy z klientów podłączonych do serwera oczekują na ponowne uruchomienie po aktualizacji do nowej wersji oprogramowania,
29. serwer centralnej administracji ma być wyposażony w wygodny mechanizm zarządzania licencjami, który umożliwi sumowanie liczby licencji nabytych przez użytkownika. Dodatkowo serwer ma informować o tym, ilu stanowiskową licencję posiada użytkownik i stale nadzorować ile licencji spośród puli nie zostało jeszcze wykorzystanych,
30. w sytuacji, gdy użytkownik wykorzysta wszystkie licencje, które posiada po zakupie oprogramowania, administrator po zalogowaniu się do serwera poprzez konsolę administracyjną musi zostać poinformowany o tym fakcie za pomocą okna informacyjnego,
31. możliwość tworzenia repozytorium aktualizacji na serwerze centralnego zarządzania i udostępniania go przez wbudowany serwer http,
32. aplikacja musi posiadać funkcjonalność, która umożliwi dystrybucję aktualizacji za pośrednictwem szyfrowanej komunikacji (za pomocą protokołu https),
33. do celu aktualizacji za pośrednictwem protokołu https nie jest wymagane instalowanie dodatkowych zewnętrznych usług jak IIS lub Apache zarówno od strony serwera aktualizacji jak i klienta,
34. dostęp do kwarantanny klienta ma być z poziomu systemu centralnego zarządzania,
35. możliwość przywrócenia lub pobrania zainfekowanego pliku ze stacji klienckiej przy wykorzystaniu centralnej administracji,

36. administrator ma mieć możliwość przywrócenia i wyłączenia ze skanowania pliku pobranego z kwarantanny stacji klienckiej,
37. podczas przywracania pliku, administrator ma mieć możliwość zdefiniowania kryteriów dla plików, które zostaną przywrócone w tym minimum: zakres czasu z dokładnością co do minuty kiedy wykryto daną infekcję, nazwa danego zagrożenia, dokładna nazwa wykrytego obiektu oraz zakres minimalnej i maksymalnej wielkości pliku z dokładnością do jednego bajta,
38. możliwość utworzenia grup, do których przynależność jest aplikowana dynamicznie na podstawie zmieniających się parametrów klientów w tym minimum w oparciu o: wersję bazy sygnatur wirusów, maskę wersji bazy sygnatur wirusów, nazwę zainstalowanej aplikacji, dokładną wersję zainstalowanej aplikacji, przynależność do domeny lub grupy roboczej, przynależność do serwera centralnego zarządzania, przynależności lub jej braku do grup statycznych, nazwę komputera lub jej maskę, adres IP, zakres adresów IP, przypisaną politykę, czas ostatniego połączenia z systemem centralnej administracji, oczekiwania na restart, ostatnie zdarzenie związane z wirusem, ostatnie zdarzenie związane z usługą programu lub jego procesem, ostatnie zdarzenie związane ze skanowaniem na żądanie oraz z nieudanym leczeniem podczas takiego skanowania, maską wersji systemu operacyjnego oraz flagą klienta mobilnego,
39. podczas tworzenia grup dynamicznych, parametry dla klientów można dowolnie łączyć oraz dokonywać wykluczeń pomiędzy nimi,
40. utworzone grupy dynamiczne mogą współpracować z grupami statycznymi,
41. możliwość definiowania administratorów o określonych prawach do zarządzania serwerem administracji centralnej (w tym możliwość utworzenia administratora z pełnymi uprawnieniami lub uprawnienia tylko do odczytu).
42. w przypadku tworzenia administratora z niestandardowymi uprawnieniami możliwość wyboru modułów, do których ma mieć uprawnienia: zarządzanie grupami, powiadomieniami, politykami, licencjami oraz usuwanie i modyfikacja klientów, zdalna instalacja, generowanie raportów, usuwanie logów, zmiana konfiguracji klientów, aktualizacja zdalna, zdalne skanowanie klientów, zarządzanie kwarantanna na klientach,
43. możliwość synchronizowania użytkowników z Active Directory w celu nadania uprawnień administracyjnych do serwera centralnego zarządzania,
44. wszystkie działania administratorów zalogowanych do serwera administracji centralnej mają być logowane,
45. możliwość uruchomienia panelu kontrolnego dostępnego za pomocą przeglądarki internetowej,
46. panel kontrolny musi umożliwiać administratorowi wybór elementów monitorujących, które mają być widoczne,
47. administrator musi posiadać możliwość tworzenia wielu zakładek, w których będą widoczne wybrane przez administratora elementy monitorujące,
48. elementy monitorujące muszą umożliwiać podgląd w postaci graficznej co najmniej: bieżącego obciążenia serwera zarządzającego, statusu serwera zarządzającego, obciążenia bazy danych z której korzysta serwer zarządzający, obciążenia komputera, na którym zainstalowana jest usługa serwera zarządzającego, informacji odnośnie komputerów z zainstalowaną aplikacja antywirusową, a które nie są centralnie zarządzane, podsumowania modułu antyspamowego, informacji o klientach znajdujących się w poszczególnych grupach, informacji o klientach z największą ilością zablokowanych stron internetowych, klientach, na których zostały zablokowane urządzenia zewnętrzne, informacje na temat greylistingu, podsumowania wykorzystywanych systemach operacyjnych, informacje odnośnie spamu sms, zagrożeń oraz ataków sieciowych,
49. administrator musi posiadać możliwość maksymalizacji wybranego elementu monitorującego,
50. możliwość włączenia opcji pobierania aktualizacji z serwerów producenta z opóźnieniem,
51. możliwość przywrócenia baz sygnatur wirusów wstecz (tzw. Rollback),
52. aplikacja musi mieć możliwość przygotowania paczki instalacyjnej dla stacji klienckiej, która będzie pozbawiona wybranej funkcjonalności,
53. wsparcie dla protokołu IPv6,

54. administrator musi posiadać możliwość centralnego, tymczasowego wyłączenia wybranego modułu ochrony na stacji roboczej,
55. centralne tymczasowe wyłączenie danego modułu nie może skutkować koniecznością restartu stacji roboczej,
56. aplikacja musi posiadać możliwość natychmiastowego uruchomienia zadania znajdującego się w harmonogramie bez konieczności oczekiwania do jego zaplanowanego czasu,
57. aplikacja do administracji centralnej musi umożliwiać utworzenie nośnika, za pomocą którego będzie istniała możliwość przeskanowania dowolnego komputera objętego licencją przed startem systemu,
58. administrator musi posiadać możliwość określenia ilości jednoczesnych wątków instalacji centralnej oprogramowania klienckiego.

6. **Zakup mobilnych stanowisk administracyjnych typu B – szt. 4 w ukompletowaniu:**
   - Procesor: CPU charakteryzujący się posiadaniem min. 2 rdzeni fizycznych z możliwością obsługi co najmniej dwóch wątków przez każdy rdzeń, o częstotliwości taktowania co najmniej 3,1 GHz. Wykonanego w technologii x86 64 bit, pamięci podręcznej L3 min 4 MB, wyposażony w wirtualizację sprzętową typ. Instrukcja VT-x lub podobna, który w testach CPU Benchmarks osiąga średni wynik powyżej 4900 pkt. (źródło www.cpubenchmark.net), przykładowym procesorem spełniającym w/w kryteria jest i7 5557U @ 3.1 GHz),
   - Pamięć RAM: min. 16 GB,
   - Wyświetlacz: z podświetlaniem LED w technologii IPS, przekątna ekranu 13,3", rozdzielczość min. 2560 x 1600 pix, min. 227 pix na cal (ppi),
   - Dysk HDD w technologii SSD o rozmiarze min. 1 TB,
   - Interfejs sieciowy Ethernet 1Gbit/s (RJ45),
   - System Operacyjny: OS X Yosemite lub równoważny zgodnie z opisem określonym w pkt. 5
   - Dodatkowy zasilacz zgodny z interfejsem MagSafe 2,
   - Oprogramowanie biurowe: Microsoft Office 2011 (Mac) lub równoważny zgodnie z opisem określonym w pkt. 5
   - Oprogramowanie do wirtualizacji: VMware Fusion 8 Pro lub równoważny zgodnie z opisem określonym w pkt. 5

- Oprogramowanie antywirusowe z modułem zapory (Firewall): ESET ENDPOINT SECURITY for Mac OS X z licencją na okres 3 lat lub równoważny zgodnie z opisem określonym w pkt. 5

Załącznik nr 2 do SIWZ
nr sprawy 252/BŁiI/15/MT

.....
pieczęć wykonawcy

FORMULARZ OFERTOWY

dotyczy postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na dostawę narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT, sprawa nr 252/BŁiI/15/MT

1. Pełna nazwa wykonawcy,
   .....
2. Adres, nr telefonu, nr faksu .....
3. Imiona, nazwiska osoby / osób upoważnionych do kontaktu ze strony Wykonawcy
   .....

4. Oferujemy realizację przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia stanowiącym Załącznik nr 1 do SIWZ za:

Cena oferty brutto wynosi ..... zł (*kwota z pkt. a) + kwota z pkt. b) + wartość podatku VAT z pkt. b)*

w tym,

a) Cena oferty brutto wynosi .....zł (*dotyczy urządzeń wskazanych w pkt. 1-4 Załącznika nr 1do SIWZ*)

słownie :.....

b) Cena oferty netto wynosi .....zł (*dotyczy urządzeń wskazanych w pkt. 5 i 6 Załącznika nr 1do SIWZ*)

słownie :.....
VAT .....%
Wartość podatku VAT wynosi ..... zł

słownie :.....

Uwaga:
1) Kryterium oceny ofert „Cena oferty brutto"- kwota z pkt. a) + kwota z pkt. b) + wartość podatku VAT z pkt. b)
2) Ceny należy podać z zaokrągleniem do dwóch miejsc po przecinku.

Oświadczamy, że wybór oferty będzie prowadzić/nie będzie prowadzić* do powstania u Zamawiającego obowiązku podatkowego w przypadku urządzeń wskazanych w pkt. 5 i 6 Złącznika nr 1 do SIWZ.

Przedłużamy okres gwarancji:
- serwer - o ..... miesięcy ponad wymagane minimalne (min. 36 miesięcy)
- terminal – o ..... miesięcy ponad wymagane minimalne (min. - 36 miesięcy)
- monitor 28" - o ..... miesięcy ponad wymagane minimalne (min. 36 miesięcy)

- stanowiska administracyjne - o ..... miesięcy ponad wymagane minimalne (min. 24 miesiące)
- stanowiska do prezentacji - o ..... miesięcy ponad wymagane minimalne (min. 24 miesiące)
- monitor 50'' - o ..... miesięcy ponad wymagane minimalne (min. 24 miesiące)
- mobilne stanowiska typ A i typ B- o ..... miesięcy ponad wymagane minimalne (min. 12 miesiące)

Uwaga:
1. Przedłużenie okresu gwarancji należy podać w pełnych 6 miesięcy
2. W każdym urządzeniu wykonawca może uzyskać maksymalnie 2 punkty za okres gwarancji.
3. W przypadku wpisania cyfry 0 (lub brak wpisu) Zamawiający uzna, że Wykonawca nie przedłuża terminu wsparcia oraz oferuje minimalny okres gwarancji określone odpowiednio w załączniku nr 3 do umowy.

5.Akceptujemy warunki płatności opisane w projekcie umowy, stanowiącym załącznik nr 5 do SIWZ.

6. Oświadczamy, że spełniamy warunki udziału w postępowaniu określone w art. 22 ust. 1 ustawy Pzp, na potwierdzenie spełniania tych warunków do oferty załączamy dokumenty wymagane w SIWZ.

7. Przedmiot zamówienia zrealizujemy w terminie wskazanym w Rozdziale V SIWZ.

8. Oświadczamy, że:
a) zapoznaliśmy się z treścią SIWZ i nie wnosimy do niej zastrzeżeń,
b) otrzymaliśmy konieczne informacje do przygotowania oferty,
c) uważamy się za związanych niniejszą ofertą przez czas wskazany w specyfikacji istotnych warunków zamówienia,
d) akceptujemy zawarty w Załączniku nr 5 projekt umowy w sprawie zamówienia publicznego i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na wyżej wymienionych warunkach, w miejscu i terminie wskazanym przez Zamawiającego,
f) ofertę składamy na ..... kolejno ponumerowanych i podpisanych stronach.

9. Oświadczamy, że następujące części zamówienia zamierzam powierzyć podwykonawcy (om)*:.....
.....

..... , dnia .....r.
Miejscowość

.....
Podpis osoby (osób) upoważnionej do występowania w imieniu Wykonawcy
(Pożądany czytelny podpis albo podpis i pieczątka z imieniem i nazwiskiem)

Załącznik nr 3 do SIWZ
nr sprawy 252/BŁiI/15/MT

.....
pieczęć wykonawcy

OŚWIADCZENIE
w postępowaniu nr 252/BŁiI/15/MT

Przystępując do udziału w postępowaniu o zamówienie publiczne na:

dostawę narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT

oświadczamy, że nie ma podstaw do wykluczenia nas z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 ustawy Pzp

....., dn. .....

.....
(podpis i pieczęć upoważnionego przedstawiciela)

Załącznik nr 4 do SIWZ
Nr sprawy 252/BŁiI/15/MT

(pieczęć Wykonawcy)

Informacja

o której mowa w art. 26 ust. 2d ustawy Prawo zamówień publicznych

Przystępując do udziału w postępowaniu o zamówienie publiczne na **dostawę narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT (sprawa nr 252/BŁiI/15/MT),** na podstawie art. 26 ust. 2d ustawy Pzp informuję, że nie należę do grupy kapitałowej / należę do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt. 5, w skład której wchodzą niżej wymienione podmioty: *

Lp.	Dane podmiotu

* niepotrzebne skreślić

....., dn. .....

.....
(podpis i pieczęć upoważnionego przedstawiciela)

Załącznik nr 5 do SIWZ
Nr sprawy 252/BŁiI/15/MT

PROJEKT UMOWY

Egz. nr ____

U M O W A nr - ...../...../BŁiI/15/.....

zawarta w Warszawie w dniu ..... 2015 roku

pomiędzy:

Skarbem Państwa - Komendantem Głównym Policji z siedzibą w Warszawie przy ul. Puławskiej 148/150, zwanym w treści umowy **„Zamawiającym"**, reprezentowanym przez:

1.	Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji
2.	Z-cę Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji

oraz przy kontrasygnacie

1.....	Zastępcy Dyrektora Biura Finansów Komendy Głównej Policji
2.....	Naczelnik Wydziału Księgowości Komendy Głównej Policji

a firmą ..... z siedzibą w ..... przy ul. ..... wpisaną do Krajowego Rejestru Sądowego prowadzonego przez ..... pod numerem KRS .....NIP ....., REGON ..... zwaną w treści umowy **„Wykonawcą"** reprezentowaną przez:

....

Zwanymi dalej łącznie „stronami".

Umowa zostaje zawarta na podstawie przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego – numer postępowania ..... z zastosowaniem przepisów ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907, z późn. zm.)
Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1

Przedmiot umowy

1. Przedmiotem umowy jest zakup i dostawa narzędzi informatycznych do pracy Zespołu Reagowania na Incydenty Komputerowe POL-CERT.
2. Szczegółowy opis Przedmiotu umowy zawiera Załącznik nr 1.
3. Na Przedmiot umowy określony w ust. 1 składają się następujące czynności:
   1) sprzedaż i dostarczenie przez Wykonawcę do siedziby Zamawiającego Przedmiot umowy zgodnie z Załącznikiem nr 1,
   2) przekazanie przez Wykonawcę dokumentów licencyjnych/kodów aktywacyjnych/kluczy licencyjnych/haseł do oprogramowania wraz z możliwością aktualizacji określonych w Załączniku nr 1.
   3) udzielenie gwarancji i zapewnienie serwisu gwarancyjnego na zasadach określonych w Umowie i Załączniku nr 3,
   4) dostarczenie pełnej dokumentacji (tj. instrukcji obsługi) standardowo sporządzanej przez producentów sprzętu sporządzonej w języku polskim lub j. angielskim oraz kart gwarancyjnych do Przedmiotu umowy.
4. Strony zgodnie oświadczają , że dokumentacja o której mowa w ust. 3 pkt. 5 nie stanowi utworu w rozumieniu ustawy o prawie autorskim i prawach pokrewnych.

5. Na podstawie Umowy Wykonawca zobowiązuje się przenieść na Zamawiającego własność Przedmiotu umowy i wydać mu go na zasadach określonych w § 4, a Zamawiający zobowiązuje się odebrać Przedmiot umowy na zasadach określonych w Załączniku nr 2.
6. Specyfikację ilościowo-cenową zawiera Załącznik nr 4.
7. Ilekroć w dalszych postanowieniach umowy, mowa jest o terminalach, stanowiskach, serwerach, monitorach, oprogramowaniu, urządzeniach należy przez to rozumieć Przedmiot umowy określony w Załączniku nr 1.
8. Postanowienia Umowy obowiązują z dniem zawarcia.

§ 2
Organizacja projektu

1. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Zamawiający na Kierownika Projektu wyznacza nw. przedstawiciela:
   ..... - Biuro Łączności i Informatyki Komendy Głównej Policji
2. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Wykonawca na Kierownika Projektu wyznacza nw. przedstawiciela:
   .....
3. Kierownicy Projektu o których mowa w ust. 1 i 2, odpowiednio ze strony Zamawiającego i Wykonawcy, odpowiadają za nadzór nad wykonaniem Przedmiotu umowy zgodnie z wymaganiami, w założonym terminie, w ramach określonego budżetu, przy wykorzystaniu dostępnych zasobów i środków.
4. Kierownicy Projektu upoważnieni są do podejmowania decyzji i akceptacji zmian dotyczących realizacji Przedmiotu umowy, za wyjątkiem decyzji wymagających formy aneksu.
5. Obie Strony mogą zmienić swoich przedstawicieli w organizacji projektu informując drugą Stronę, z co najmniej 2-dniowym (dni robocze) wyprzedzeniem. Zmiana taka nie wymaga aneksu do Umowy.
6. Za dzień roboczy uważa się każdy dzień od poniedziałku do piątku w godzinach 8.15 – 16.15 z wyłączeniem dni ustawowo wolnych od pracy w Polsce.

§ 3
Wykonanie Umowy

1. Wykonawca zobowiązuje się wykonać Umowę przy zachowaniu najwyższej staranności uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami wiedzy i stosowanymi normami technicznymi.
2. Strony zgodnie oświadczają, iż wydanie Przedmiotu umowy następuje w dniu dostarczenia przez Wykonawcę Przedmiotu umowy w miejsce i na zasadach wskazanych w Załączniku nr 2.
3. Wykonawca oświadcza, że dostarczony Przedmiot umowy będzie fabrycznie nowy, wolny od wad fizycznych i prawnych , wyprodukowany w 2015 r. oraz nie toczy się żadne postępowanie, którego przedmiotem jest Przedmiot umowy. Nie jest on obciążony zastawem, zastawem rejestrowym ani zastawem skarbowym ani żadnymi innymi ograniczonymi prawami rzeczowymi.
4. Wykonawca jest zobowiązany do spełnienia wymogów w zakresie zapewnienia efektywności energetycznej dostarczanych urządzeń, wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (WE) 106/2008 z dnia 15.01.2008 w sprawie wspólnotowego programu znakowania efektywności energetycznej urządzeń biurowych - ***Energy Star***
5. Dostarczony sprzęt będzie posiadać oznakowanie **CE** – ***Conformite Europeenne,***
6. Oprogramowanie będące wyposażeniem sprzętu dostarczonego w ramach Przedmiotu Umowy musi być dostarczone w oryginalnych opakowaniach producenta, z dołączoną licencją;

§ 4
Termin i warunki dostawy

1. Wykonawca zobowiązuje się dostarczyć Przedmiot umowy **do 18 grudnia 2015 r.**
2. Za termin dostarczenia Przedmiotu umowy przyjmuje się datę podpisania bez zastrzeżeń przez przedstawicieli Stron protokołu odbioru **ilościowego**, którego wzór stanowi Załącznik nr 5.
3. Przedmiot umowy podlegać będzie odbiorom. Szczegółowe zasady odbiorów Przedmiotu umowy zawiera Załącznik nr 2.
4. Wszystkie czynności związane z odbiorami muszą zakończyć się w terminie wskazanym w ust. 1.

5. Wykonawca jest zobowiązany do ścisłej współpracy z Zamawiającym i niezwłocznego informowania o wszelkich okolicznościach mogących mieć wpływ na terminowość umowy.
6. Wykonawca ponosi pełną odpowiedzialność za ewentualne uszkodzenia urządzeń do czasu ich odbioru przez Zmawiającego na zasadach określonych w Załączniku nr 2.
7. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób uprawnionych do wykonywania czynności serwisowych oraz osób upoważnionych do realizacji Umowy. W celu zapewnienia kontroli osób uzyskujących dostęp do policyjnych zasobów, w tym Aktywów Teleinformatycznych, Wykonawca wraz z listą osób dostarczy:
   1. aktualne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych stanowiących tajemnicę służbową oznaczoną klauzulą „poufne",
   2. oświadczenie o zachowaniu poufności dla każdej osoby realizującej Umowę, którego wzór określa Załącznik nr 9 do Umowy.
8. Zamawiający dopuści do realizacji Przedmiotu umowy jedynie osoby spełniające warunki określone w ust. 7.

§ 5
Płatności

1. Wartość Przedmiotu umowy, określonego w § 1 Strony ustalają na kwotę: netto .....00/100 zł (słownie: ..... zł 00/100), co wraz z podatkiem VAT stanowi łącznie ..... zł brutto (słownie: ..... zł 00/100), w tym:
   Wartość Przedmiotu umowy brutto obejmuje wszelkie koszty związane z realizacją Umowy z uwzględnieniem podatku od towarów i usług VAT, innych opłat i podatków, opłat celnych, kosztów dokumentacji, kosztów opakowania oraz ewentualnych upustów i rabatów, skalkulowanych z uwzględnieniem kosztów dostawy (transportu) do określonej Umową lokalizacji.
2. Zamawiający opłaci należność za wykonanie Przedmiotu umowy na podstawie prawidłowo wystawionej przez Wykonawcę faktury, zgodnie z Załącznikiem nr 4
3. Kwotę w wysokości ..... tj. podatek od towaru i usług VAT w stawce .....% VAT, stanowiącą należności od kwoty wynagrodzenia, wymienionego w Załączniku nr 4 poz. ....., Zamawiający pokryje na konto właściwego Urzędu Skarbowego w przypadku powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami ustawy z dnia 9 kwietnia 2015 r. o zmianie ustawy o podatku od towarów i usług oraz ustawy Prawo zamówień publicznych (Dz. U. z 2015 r. poz.605).
4. Wykonawca wystawi fakturę, wskazując jako płatnika:

Komenda Główna Policji
02-624 Warszawa, ul. Puławska 148/150
NIP 521-31-72-762, REGON 012137497

5. Podstawę do wystawienia faktury stanowi podpisany bez zastrzeżeń przez przedstawicieli Zamawiającego i Wykonawcy protokół odbioru **ilościowego**, którego wzór stanowi Załącznik nr 5.
6. Płatność za realizację Przedmiotu umowy dokonana będzie przelewem bankowym na rachunek Wykonawcy, wskazany na prawidłowo wystawionej fakturze, w terminie 30 dni od daty dostarczenia faktury do siedziby Biura Łączności i Informatyki KGP, ul. Wiśniowa 58, 02-520 Warszawa.
7. Za termin zapłaty przyjmuje się datę obciążenia przez bank rachunku Zamawiającego.
8. Zamawiający upoważnia Wykonawcę do wystawienia faktur bez podpisu Zamawiającego.
9. Wszelkie rozliczenia finansowe między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
10. Przed zawarciem Umowy Wykonawca wniósł zabezpieczenie należytego wykonania Umowy w wysokości 10% ceny całkowitej podanej w ofercie tj. kwotę ..... zł (słownie: ..... zł i 00/100).
11. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone w następujących terminach:
    a) 70% zabezpieczenia należytego wykonania Umowy tj. kwotę ..... zł, gwarantującą zgodne z Umową wykonanie Przedmiotu umowy, w terminie 30 dni po ostatecznym, bezusterkowym odbiorze Przedmiotu umowy,
    b) 30% zabezpieczenia należytego wykonania Umowy tj. kwotę ..... zł, nie później niż 15 dni po upływie okresu rękojmi za wady.
12. Wniesione przez Wykonawcę zabezpieczenie jest przeznaczone na pokrycie roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, w tym roszczeń z tytułu rękojmi za wady.
13. Wykonawca zobowiązuje się, że w przypadku wniesienia zabezpieczenia w gwarancjach bankowych lub ubezpieczeniowych, gwarancja bankowa lub ubezpieczeniowa będzie nieodwołalna, bezwarunkowa, płatna na każde pierwsze żądanie Zamawiającego.

14. Jeżeli z uwagi na przedłużenie terminu realizacji umowy, niezależnie od przyczyn tego przedłużenia, zabezpieczenie wniesione w formie gwarancji bankowych, ubezpieczeniowych lub poręczeniach wygasałoby przed upływem przedłużonego terminu realizacji umowy, Wykonawca na 7 dni roboczych przed wygaśnięciem tego zabezpieczenia przedstawi Zamawiającemu stosowny aneks do gwarancji/poręczenia lub nową gwarancję/poręczenie lub wpłaci odpowiednie zabezpieczenie w formie pieniądza. Jeżeli Wykonawca nie wypełni tego obowiązku Zamawiający może zażądać od gwaranta/poręczyciela wpłaty z gwarancji/poręczenia i zaliczyć uzyskaną w ten sposób kwotę na poczet zabezpieczenia.
15. Wykonawca oświadcza, że wyraża zgodę na bezpośrednie potrącenie przez Zamawiającego z zabezpieczenia wszelkich należności powstałych w wyniku niewykonania lub nienależytego wykonania umowy.

§ 6
Gwarancja

1. Bieg okresu gwarancji rozpocznie się od daty podpisania bez zastrzeżeń protokołu odbioru ilościowego.
2. Warunki gwarancyjne i serwisowe określa Załącznik nr 3.

§ 7
Kary

1. Wykonawca odpowiada za szkodę, wyrządzoną Zmawiającemu, w tym również za szkodę wyrządzoną przez osoby, którymi Wykonawca posłużył się przy wykonywaniu Umowy, chyba że szkoda została spowodowana działaniem „Siły Wyższej", wyłączną winą Zamawiającego lub osoby trzeciej, za którą Wykonawca nie ponosi odpowiedzialności.
2. W przypadku niewykonania lub nienależytego wykonania Umowy, Wykonawca zobowiązuje się zapłacić Zamawiającemu następujące kary umowne:
   1) 10% wartości całkowitej Przedmiotu umowy w razie odstąpienia przez Wykonawcę lub Zamawiającego od Umowy z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy,
   2) 0,15% wartości całkowitej Przedmiotu umowy za każdy rozpoczęty dzień opóźnienia w wykonaniu Przedmiotu umowy;
   3) 0,15% wartości całkowitej Przedmiotu umowy z tytułu przekroczenia wymaganego czasu naprawy gwarancyjnej o której mowa w Załączniku nr 3 za każdy dzień przekroczenia.
3. Zapłata kar umownych, o których mowa w ust. 2 pkt. 2 nie zwalnia Wykonawcy z obowiązku wykonania Przedmiotu umowy.
4. Prawo naliczenia kar umownych, o których mowa w ust. 2 nie ma zastosowania w przypadku gdy opóźnienie wynika z winy Zamawiającego.
5. Zamawiający jest uprawniony do potrącenia naliczonych kar umownych z wynagrodzenia przysługującego Wykonawcy. Doręczenie Wykonawcy, wystawionej przez Zamawiającego noty obciążeniowej, w której określono: kwotę naliczonych kar umownych, podstawę ich naliczenia oraz wprowadzono oświadczenie o ich potrąceniu z wynagrodzenia, zastępuje wezwanie do zapłaty oraz oświadczenie Zamawiającego o potrąceniu kar umownych."
6. Niezależnie od kar umownych określonych w ust. 2, Stronom przysługuje prawo dochodzenia odszkodowania na zasadach ogólnych prawa cywilnego, jeżeli poniesiona szkoda przekroczy wysokość zastrzeżonych kar umownych.
7. Kary umowne podlegają łączeniu.
8. Żadna Strona nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań w ramach Umowy, jeżeli takie niewykonanie lub nienależyte wykonanie jest wynikiem „Siły Wyższej".
9. W rozumieniu Umowy, „Siła Wyższa" oznacza okoliczności pozostające poza kontrolą Strony i uniemożliwiające lub znacznie utrudniające wykonanie przez tę Stronę jej zobowiązań, których nie można było przewidzieć w chwili zawierania Umowy, ani im zapobiec przy dołożeniu należytej staranności.
10. Za „Siłę Wyższą" nie uznaje się niedotrzymania zobowiązań przez kontrahenta – dostawcę Wykonawcy.
11. W przypadku zaistnienia okoliczności „Siły Wyższej", Strona, która powołuje się na te okoliczności, niezwłocznie zawiadomi druga Stronę na piśmie o jej zaistnieniu i przyczynach.
12. W razie zaistnienia „Siły Wyższej" wpływającej na termin realizacji Umowy, Strony zobowiązują się w terminie 14 (czternastu) dni od dnia zawiadomienia, o którym mowa w ust. 11, ustalić nowy termin wykonania Umowy lub ewentualnie podjąć decyzję o odstąpieniu od Umowy za porozumieniem Stron.

§ 8
Licencje na Oprogramowanie

1. Wykonawca gwarantuje, iż z chwilą podpisania protokołu odbioru ilościowego bez uwag, Zamawiający w ramach wynagrodzenia wskazanego w § 5 ust. 1 uzyskuje prawo do korzystania z oprogramowania oraz ich aktualizacji, na podstawie bezterminowej, niewyłącznej licencji udzielonej przez producenta oprogramowania, której warunki tenże producent dołączył do oprogramowania. Przedmiotową licencję można wypowiedzieć z zachowaniem 10-letniego okresu wypowiedzenia, ze skutkiem na koniec roku kalendarzowego.
2. Wykonawca uzyskał zgodę producenta na korzystanie przez Zamawiającego z oprogramowania określonego w Załączniku nr 1, w tym na przekazywanie dokumentów zawierających warunki licencji.
3. W okresie od dnia dostarczenia do Zamawiającego oprogramowania, o którym mowa w § 1 ust. 1, w sposób określony w Umowie, do dnia podpisania protokołu odbioru ilościowego, Wykonawca zapewni Zamawiającemu korzystanie z tego oprogramowania na warunkach licencji, bez pobierania z tego tytułu dodatkowego wynagrodzenia.
4. Przekazanie Zamawiającemu licencji na oprogramowanie, określone w § 1 ust. 1 Umowy, następuje z chwilą podpisania przez Strony protokołu odbioru ilościowego,
9. Dostarczone licencje będą wolne od roszczeń osób trzecich z tytułu naruszenia praw autorskich oraz innych praw pokrewnych a w szczególności patentów, zarejestrowanych znaków i wzorów w związku z użytkowaniem bez możliwości ich wypowiedzenia.
10. Wykonawca oświadcza i gwarantuje, że Oprogramowanie i jego aktualizacje, ani korzystanie z niego przez Zamawiającego zgodnie z Umową, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów,
11. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z oprogramowaniem i jego aktualizacjami, w tym zarzucających naruszenie praw własności intelektualnej, Wykonawca podejmie wszelkie działania mające na celu zażegnanie sporu i poniesie w związku z tym wszelkie koszty, w tym koszty zastępstwa procesowego od chwili zgłoszenia roszczenia oraz koszty odszkodowań. W szczególności, w razie wytoczenia przeciwko Zamawiającemu powództwa z tytułu naruszenia praw własności intelektualnej, Wykonawca wstąpi do postępowania w charakterze strony pozwanej, a w razie braku takiej możliwości wystąpi z interwencją uboczną po stronie Zamawiającego.
12. Ponadto, jeśli używane oprogramowanie i jego aktualizacje stanie się przedmiotem jakiegokolwiek powództwa Strony lub osoby trzeciej o naruszenie praw własności intelektualnej, jak wymieniono powyżej, Wykonawca może na swój własny koszt wybrać jedno z poniższych rozwiązań:
    a) uzyskać dla Zamawiającego prawo dalszego użytkowania oprogramowania i jego aktualizacji lub
    b) zmodyfikować oprogramowanie i jego aktualizacje tak, żeby było zgodne z Umową, ale wolne od jakichkolwiek wad lub roszczeń osób trzecich.
13. Strony potwierdzają, że żadne z powyższych postanowień nie wyłącza:
    a) możliwości dochodzenia przez Zamawiającego odszkodowania na zasadach ogólnych kodeksu cywilnego lub wykonania uprawnień przez Zamawiającego wynikających z innych ustaw, ani
    b) dochodzenia odpowiedzialności z innych tytułów określonych w Umowie, a w szczególności w § 7.

§ 9
Zmiany Umowy

1. Strony przewidują możliwość dokonywania zmian w treści Umowy w stosunku do treści oferty Wykonawcy w sytuacji gdy:
    a) powstała możliwość zastosowania nowszych lub korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili zawarcia Umowy, nie powodujących zmiany Przedmiotu umowy i nie powodujących podwyższenia ceny;
    b) powstała możliwość zastosowania nowszych lub korzystniejszych dla Zamawiającego rozwiązań w zakresie modelu/typu sprzętu w przypadku zakończenia produkcji, braku dostępności na rynku pod warunkiem, że będzie posiadał parametry nie gorsze od oferowanego modelu/typu i nie spowoduje podwyższenia ceny;
    c) po zawarciu Umowy doszło do wydłużenia okresu gwarancyjnego przez producenta;
    d) niezbędna jest zmiana sposobu wykonania zobowiązania o ile zmiana taka jest korzystna dla Zamawiającego oraz konieczna w celu prawidłowego wykonania Umowy.
2. Zmiany, o których mowa w ust. 1, wymagają zgody obu stron i muszą być dokonywane w formie pisemnej pod rygorem nieważności w postaci aneksu.

§ 10
Odstąpienie od umowy

1. Zamawiającemu przysługuje prawo odstąpienia od umowy w sytuacji gdy:

   a) wystąpiła istotna zmiana okoliczności powodująca, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy. Zamawiający może odstąpić od umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach,
   b) opóźnienia w wykonaniu Przedmiotu umowy trwającego dłużej niż **5** dni. Zamawiający może, niezależnie od kar umownych przewidzianych w ust. 2 powyżej odstąpić od umowy bez obowiązku wyznaczania dodatkowego terminu. Oświadczenie o odstąpieniu o którym mowa, winno być złożone przez Zamawiającego w terminie 30 dni roboczych od dnia w którym upłynął **2** dniowy termin opóźnienia w stosunku do terminu wskazanego w § 4 ust. 1.
   c) Wykonawca dostarczył Przedmiot umowy, który nie spełnia wymogów określonych w Załączniku nr 1 lub dostawy Sprzętu bez wymaganych Umową dokumentów (licencji na Oprogramowanie). Oświadczenie o odstąpieniu, winno być złożone przez Zamawiającego w terminie 30 dni roboczych od dnia dostarczenia przez Wykonawcę Sprzętu niespełniającego wymogów określonych w Załączniku nr 1 Umowy lub dostarczenia Sprzętu bez wymaganych dokumentów o których mowa w § 1 ust 3 pkt. 3, 4 i 5.
   d) w wypadku, gdy łączna wysokość kar umownych przekroczy 100% łącznego wynagrodzenia brutto, określonego w § 5 ust. 1 Umowy, Zamawiający może od umowy odstąpić w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach bez wyznaczania dodatkowego terminu.

2. Odstąpienie od Umowy powinno nastąpić poprzez złożenie stosownego oświadczenia woli w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie. Odstąpienie wywołuje skutki z chwilą doręczenia, z tym, że dla zachowania terminu na odstąpienie wystarczy wysłanie oświadczenia o odstąpieniu przesyłką rejestrowaną na adres Strony przeciwnej wskazany w komparycji Umowy albo na aktualny adres KRS.
3. W przypadku odstąpienia od realizacji Umowy Wykonawca uprawniony jest do otrzymania wynagrodzenia za wykonane prace oraz świadczone usługi należne do dnia odstąpienia od Umowy.
4. Odstąpienie od Umowy nie powoduje wygaśnięcia roszczeń o zapłatę kar umownych powstałych w czasie obowiązywania Umowy (w tym roszczenia o zapłatę kary umownej z powodu odstąpienia od Umowy).

§ 11
Inne postanowienia

1. Przy prowadzeniu korespondencji w sprawach związanych z realizacją Przedmiotu umowy obowiązywać będzie forma pisemna.
2. W razie pilnej potrzeby zawiadomienia mogą być przesyłane faksem z pisemnym potwierdzeniem ich otrzymania.
3. Ustala się następujące adresy, numery faksów i telefonów:

   Adres Wykonawcy dla potrzeb korespondencji i składania zawiadomień:
   .....
   .....
   tel. .....
   fax .....
   Adres Zamawiającego dla potrzeb korespondencji składania zawiadomień:
   Biuro Łączności i Informatyki KGP
   02-520 Warszawa, ul. Wiśniowa 58
   fax./22/ 60-158-73

§ 11
Postanowienia końcowe

1. Wykonawca nie może bez pisemnej – pod rygorem nieważności – i uprzedniej zgody Zamawiającego przenieść na osobę trzecią żadnej wierzytelności wynikającej z niniejszej Umowy.
2. W sprawach nieuregulowanych Umową stosuje się przepisy Kodeksu Cywilnego, ustawy Prawo Zamówień Publicznych oraz ustawy o prawie autorskim i prawach pokrewnych.

3. Sądem właściwym dla spraw Umowy jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. W przypadku zaistnienia jakichkolwiek rozbieżności pomiędzy postanowieniami zawartymi w załącznikach a warunkami ustalonymi w Umowie, wiążące są postanowienia Umowy
5. W wypadku jeżeli postanowienia kart gwarancyjnych są sprzeczne z postanowieniami umowy stosuje się postanowienia umowy.
6. Umowę sporządzono w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający i 1 (jeden) egzemplarz otrzymuje Wykonawca.
7. W przypadku zaistnienia jakichkolwiek rozbieżności pomiędzy postanowieniami zawartymi w załącznikach a warunkami ustalonymi w Umowie, wiążące są postanowienia Umowy.

Załączniki stanowiące integralną część Umowy:

1) Załącznik nr 1 - Szczegółowy opis Przedmiotu umowy,
2) Załącznik nr 2 - Zasady odbioru Przedmiotu umowy,
3) Załącznik nr 3 – Warunki gwarancyjne i serwisowe,
4) Załącznik nr 4 - Specyfikacja ilościowo-cenowa,
5) Załącznik nr 5 – Protokół odbioru ilościowego,
6) Załącznik nr 6 – Protokół odbioru jakościowego
7) Załącznik nr 7 – Zgłoszenie serwisowe,
8) Załącznik nr 8 – Wzór formularza zgłoszenia serwisowego.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1
do Umowy nr-……/……./BŁiI/15/…..

Szczegółowy opis Przedmiotu umowy
(opis przedmiotu umowy zostanie sporządzony na podstawie oferty wykonawcy)

Przedmiotem umowy jest dostawa do siedziby Zamawiającego narzędzi informatycznych do pracy zespołu reagowania na incydenty komputerowe POL-CERT.
W ramach umowy Wykonawca dostarczy sprzęt w następujących typach, ilościach i min. parametrach:

Załącznik nr 2
do Umowy nr ...../...../BŁiI/15/...

Zasady odbioru Przedmiotu umowy

I. Odbiór jakościowy

1. W celu przeprowadzenia odbioru jakościowego Wykonawca dostarczy Przedmiot umowy do Biura Łączności i Informatyki KGP w Warszawie.
2. O gotowości do odbioru jakościowego i ilościowego Wykonawca powiadomi Wydział Zarządzania Projektami BŁiI KGP faksem na numer 22 60-158-73 z co najmniej 2-dniowym wyprzedzeniem, podając:
   - numer umowy,
   - planowaną datę dostarczenia przedmiotu Umowy do odbioru jakościowego,
   - numery seryjne Przedmiotu umowy
3. Odbiór jakościowy przeprowadzony zostanie przez Komisję powołaną do odbioru Przedmiotu umowy ze strony Zamawiającego, w obecności przedstawicieli Wykonawcy w godzinach 8:15-16:15 w ciągu 2 dwóch) **dni roboczych** od daty dostarczenia Przedmiotu umowy do odbioru jakościowego.
4. Celem czynności kontrolnych prowadzonych w ramach odbioru jakościowego będzie sprawdzenie przez komisję wymagań funkcjonalnych i jakości dostarczonego Przedmiotu umowy z parametrami, funkcjonalnością opisaną w umowie,
5. W trakcie odbioru Wykonawca przekaże Zamawiającemu dokument sporządzony w języku polskim, potwierdzający nabycie przez Zamawiającego licencji/kluczy licencyjnych/kodów/haseł do oprogramowania wymienionego w Załączniku nr 1. Na dostarczonym dokumencie (licencji/kluczy) będzie określony zakres usługi wsparcia oraz termin jej obowiązywania.
6. Odbiorowi jakościowemu podlegać będzie całość Przedmiotu umowy.
7. Wykonawca jest odpowiedzialny za wniesienie i rozpakowanie do odbioru jakościowego Przedmiotu umowy.
8. Jeśli w czasie odbioru jakościowego jakikolwiek Przedmiot umowy wraz z oprogramowaniem nie będzie działał poprawnie lub nie spełni wymagań konfiguracyjnych, cała partia przeznaczona do odbioru jakościowego zostanie zwrócona Wykonawcy a cała procedura odbioru zostanie powtórzona od początku.
9. Wynik odbioru jakościowego zostanie potwierdzony podpisaniem protokołu odbioru jakościowego, którego wzór określa Załącznik nr 6.
10. Protokół odbioru jakościowego zostanie sporządzony w 4 (czterech) jednobrzmiących egzemplarzach, z których 1 (jeden) egzemplarz otrzymuje Wykonawca a 3(trzy) egzemplarze otrzymuje Zamawiający.

II. Odbiór ilościowy

1. Pozytywny wynik odbioru jakościowego – bez uwag - warunkuje przystąpienie Stron do odbiorów ilościowych Przedmiotu umowy.
2. Przed przystąpieniem do odbioru ilościowego Wykonawca zobowiązany jest do przygotowania i dostarczenia Zamawiającemu wykazu zawierającego nazwę, typ, producenta produktu, ilość, cenę jednostkową netto produktu, wartość podatku VAT wraz ze stawką podatkową, cenę jednostkową brutto produktu, cenę łączną dla danej ilości produktu oraz numery seryjne.
3. Odbiór ilościowy Przedmiotu umowy zostanie przeprowadzony w miejscu odbioru jakościowego w ciągu do 2 dni roboczych przez Komisję powołaną do odbioru Przedmiotu zamówienia ze strony Zamawiającego, w obecności przedstawicieli Wykonawcy.
4. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowego jest sprawdzenie kompletności dostarczonego produktu i potwierdzenie zgodności z ilością określoną w Umowie.
5. Wykonawca zapewni opakowanie towaru wymagane do zabezpieczenia go przed uszkodzeniem w drodze do miejsca przeznaczenia. Opakowania muszą odpowiadać normom europejskim w zakresie utylizacji i będą własnością Zamawiającego.
6. Wykonawca będzie odpowiedzialny za rozpakowanie dostarczonego produktu.
7. Wynik odbioru ilościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowego, którego wzór określa Załącznik nr 6 do Umowy.
8. Pozytywny wynik odbioru ilościowego nie zwalania Wykonawcy od odpowiedzialności za wady ujawnione w terminie późniejszym.
9. Wszystkie protokoły zostaną sporządzone w czterech (4) jednobrzmiących egzemplarzach, z czego jeden (1) otrzymuje Wykonawca, a trzy (3) Zamawiający.
10. Z chwilą podpisania przez Strony – bez uwag – protokołu odbioru ilościowego, na Zamawiającego przechodzi prawo własności Przedmiotu umowy oraz wszelkie korzyści i ciężary związane ze sprzętem oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia sprzętu.

Załącznik nr 3
do Umowy nr ...../...../BŁiI/15/...

Wymagania gwarancyjne i serwisowe

1. Okres gwarancji na cały Przedmiotu umowy wynosić będzie
   - serwer - min. 36 miesiące gwarancji ,
   - terminal – min. 36 miesięcy gwarancji
   - monitor 28" – min. 36 miesięcy gwarancji,
   - stanowiska administracyjne – min. 24 miesięcy gwarancji
   - stanowiska do prezentacji – min. 24 miesiące gwarancji
   - monitor 50" – min. 24 miesiące gwarancji
   - mobilne stanowiska typ A i typ B – min. 12 miesięcy gwarancji

   przy czym bieg okresu gwarancyjnego rozpocznie się z chwilą podpisania, bez uwag, protokołu odbioru ilościowego,
2. Gwarancja obejmuje:
   - wady materiałowe i konstrukcyjne a także niespełnienie deklarowanych przez producenta parametrów lub funkcji użytkowych,
   - naprawę wykrytych uszkodzeń, w tym wymianę uszkodzonych podzespołów na nowe,
   - usuwanie wykrytych usterek i błędów funkcjonalnych w działaniu sprzętu i oprogramowania,
3. Do przedmiotu Umowy będą dołączone karty gwarancyjne zawierające numery seryjne sprzętu, termin i warunki ważności gwarancji, zgodnie z umową, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne. Wzór kart gwarancyjnych Wykonawca dostarczy do akceptacji Zmawiającemu.
4. Zgłoszenia o awariach będą przyjmowane przez 24 godziny, 7 dni w tygodniu **(24/7)**
5. Zgłoszenie awarii drogą e-mailową w godz.18,00-8,00 muszą być potwierdzone telefonicznie przez zgłaszającego.
6. Reakcja serwisu rozumiana jako przystąpienie do usunięcia awarii lub zaistniałych nieprawidłowości nastąpi nie później niż 2 godziny od momentu zgłoszenia przez Zamawiającego drogą telefoniczną lub faksową do siedziby serwisu.
7. Wykonawca zobowiązuje się do naprawy sprzętu dostarczonego w ramach umowy w siedzibie użytkownika nie później niż w ciągu **2 dni (serwer) 7 dni (sprzęt)**od momentu zgłoszenia,
8. Całość prac związanych z dostępem do serwisowanego oprogramowania oraz Przedmiotu umowy będzie przeprowadzana przez autoryzowany serwis wykonawcy.
9. Zamawiający dopuszcza wykonanie naprawy poza siedzibą użytkownika – w tym przypadku wszelkie koszty związane z transportem sprzętu i urządzeń od i do użytkownika ponosi wykonawca a czas naprawy liczy się od dnia odebrania do dnia zwrotu naprawionego sprzętu do użytkownika.
10. Wykonawca w ramach umowy, odbierze uszkodzony sprzęt od użytkownika do naprawy. Po naprawie (w ramach umowy) dostarczy sprzęt wolny od wad do użytkownika.
11. W przypadku konieczności przeprowadzenia napraw bądź wymiany elementów zawierających dane zamawiającego – poza jego siedzibą – nośniki danych pozostają w siedzibie Zamawiającego i nie podlegają wydaniu.
12. W przypadku niewykonania naprawy w terminie podanym wyżej, na okres przedłużającej się naprawy bądź usuwania usterki, zostanie dostarczy użytkownikowi sprzęt wolny od wad, równoważny funkcjonalnie. Dostawa przedmiotowego sprzętu nastąpi nie później niż w pierwszym dniu roboczym liczonym od ostatniego dnia wyznaczonego na dokonanie naprawy gwarancyjnej.
13. W przypadku jeżeli Wykonawca nie dokona naprawy Przedmiotu umowy w terminach i na zasadach wskazanych powyżej, Zamawiający ma prawo zlecić usunięcia wady lub usterki osobie trzeciej na koszt i ryzyko Wykonawcy bez potrzeby odrębnego wezwania i bez utraty gwarancji, zachowując jednocześnie prawo do naliczenia kary umownej, na zasadach określonych w § 7 ust. 2 lit.d. (wykonanie zastępcze)
14. Dwukrotne uszkodzenie tego samego Przedmiotu umowy zaistniałe w okresie gwarancji obliguje Wykonawcę do wymiany go na nowy, wolny od wad, równoważny funkcjonalnie, – w terminie 14 dni od daty ostatniego zgłoszenia serwisowego. Okres gwarancyjny określony w pkt.1 dla wymienionego sprzętu rozpocznie się z chwilą jego dostarczenia do Zamawiającego.
15. Fakt naprawy i ewentualna wymiana sprzętu na nowy będzie każdorazowo odnotowana w karcie gwarancyjnej danego sprzętu,
16. Warunki gwarancji muszą zezwalać użytkownikowi na dokonywanie zmian w konfiguracji Przedmiotu umowy i dołączanie dodatkowych urządzeń, Taka rozbudowa nie może powodować utraty praw serwisowych do istniejącej i rozszerzonej konfiguracji danego urządzenia.
17. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień zamawiającego wynikających z rękojmi za wady,

18. Dla oprogramowania obowiązują prawa gwarancyjne producenta oprogramowania.
19. Świadczenie na rzecz Zamawiającego usług serwisu gwarancyjnego Urządzeń oraz korzystanie przez Zamawiającego z uprawnień wynikających z gwarancji zawarte jest w wynagrodzeniu, o którym mowa w § 5 ust. 1 Umowy.

Załącznik nr 4
do Umowy nr ...../..../BŁiI/15/....

Specyfikacja ilościowo – cenowa
(sporządza Wykonawca przed zawarciem umowy)

L.p.	Opis / Nazwa	Ilość	Cena jedn. netto zł.	VAT %	Cena jedn. brutto zł.	Wartość netto zł.	Wartość brutto zł.
Razem							

Załącznik nr 5
do Umowy nr .../...../BŁiI/15/...

Protokół odbioru ilościowego - wzór

Miejsce dokonania odbioru:
.....

Data dokonania odbioru:
.....

Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)

Przedmiotem odbioru ilościowego przeprowadzonego w ramach umowy nr ..... jest:

Lp.	Nazwa przedmiotu	Jednostka miary	Ilość	Nr seryjny	Wartość jednostkowa [netto]	Wartość łączna [brutto]	Dokumentacja techniczna/ instrukcja obsługi/świadectwo jakości	Uwagi
				Razem:				

Komisja przeprowadził czynności kontrolne i potwierdza/nie potwierdza kompletności dostarczonego sprzętu komputerowego i oprogramowania.

Uwagi:.....

Podpisy:

1. .....

.....

2. ..... (w imieniu Wykonawcy)

3.....

(w imieniu Zamawiającego)
*niewłaściwe skreślić

Załącznik nr 6
do Umowy nr …./…./BŁiI/15/…

Protokół odbioru jakościowego

Miejsce dokonania odbioru:
……
Data dokonania odbioru:
……
Ze strony Wykonawcy:
……
(nazwa i adres)
……
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
……
(nazwa i adres)

W ramach odbioru jakościowego, przeprowadzonego do umowy nr…… z dnia……na _____, Komisja powołana na mocy Decyzji _____z dnia _____przeprowadziła czynności kontrolne i potwierdza/nie potwierdza* zgodność jakości dostarczonego produktu z parametrami/funkcjonalnością zawartymi w opisie przedmiotu umowy.

Wynik odbioru jakościowego:
f) Pozytywny*
g) Negatywny*

Uwagi:……
……

Podpisy Komisji do odbioru przedmiotu zamówienia:

1. …… ……
2. …… (przedstawiciel Wykonawcy)
3……

*niewłaściwe skreślić

Załącznik nr 7
do Umowy nr ...../...../BŁiI/15/....

ZGŁOSZENIE SERWISOWE

Zgłoszenia serwisowe on-line:

Zgłoszenia serwisowe dokonywane będą pod adresem:

Zgłoszenia serwisowe przez e-mail:

Zgłoszenia telefoniczne /faksowe:

Załącznik nr 8
do Umowy nr ...../...../BŁiI/15/....

Formularz zgłoszeniowy - wzór

Data zgłoszenia:	
Dane zgłaszającego usterkę: Firma: ..... Adres: ..... Imię i nazwisko:..... Tel./TEL.FAX:..... e-mail:	
Dane urządzeń uszkodzonych: Nazwa:..... Model: ..... Nr seryjny: ..... Ilość :	
Opis uszkodzenia:	
Informacje dodatkowe..... ..... Podpis zgłaszającego	

Załącznik nr 9
do Umowy nr ...../...../BŁiI/15/....

.....

(imię i nazwisko)

.....

(miejsce zatrudnienia)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Stwierdzam własnoręcznym podpisem, że zobowiązuję się do nie przekazywania, nie ujawniania oraz nie wykorzystywania bez zgody Dyrektora Biura Łączności i Informatyki KGP informacji uzyskanych w trakcie wykonania umowy nr ....., zawartej w dniu ..... r. pomiędzy Komendantem Głównym Policji a ....., a nie podlegających wykluczeniu na podstawie poniższych zapisów:

1. jeżeli informacja została ujawniona publicznie przez stronę, będącą właścicielem informacji chronionej;

2. jeżeli ujawnienia informacji żąda sąd lub organ ścigania w toku prowadzonych czynności na podstawie stosownych przepisów;

3. jeżeli właściciel informacji chronionej wyrazi na to uprzednio zgodę pisemną;

4. jeżeli informacja została uzyskana od osób trzecich bez naruszenia prawnych zobowiązań o poufności informacji.

.....

(data i podpis składającego oświadczenie)