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

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

„ZATWIERDZAM"

ZASTĘPCA DYREKTORA
BIURA FINANSÓW
KOMENDY GŁÓWNEJ POLICJI
Małgorzata KUBICKA

F2F - 4367/18

Sprawa nr 189/BŁiI/18/AK/PMP

SPECYFIKACJA
ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)

Dotyczy: przetargu nieograniczonego o wartości powyżej 144.000 Euro

ogłoszonego przez Komendanta Głównego Policji na realizację zamówienia pn.:

Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management).

Warszawa, dnia 11-04- 2018 r.

Komendant Główny Policji, zwany dalej Zamawiającym, zaprasza do udziału w postępowaniu prowadzonym w trybie przetargu nieograniczonego pn ***Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management,) numer postępowania 189/BŁiI/18/AK/PMP,*** zgodnie z wymaganiami określonymi w niniejszej SIWZ.

I. INFORMACJE OGÓLNE

1. Do udzielenia przedmiotowego zamówienia stosuje się przepisy ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 t.j.), 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 2017 r. poz. 459) 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.2011.43.224 j.t.).

4. Informacje w zakresie przetwarzania danych osobowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016) zawarte są w załączniku nr 5 do niniejszego SIWZ.

II. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

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

Adres do korespondencji:
WYDZIAŁ ZAMÓWIEŃ PUBLICZNYCH i FUNDUSZY POMOCOWYCH
BIURO FINANSÓW KGP,
02-672 Warszawa, ul. Domaniewska 36/38
tel. 22-60-120-44,
faks. 22-60-118-57,
e-mail: zamowieniakgp@policja.gov.pl
strona internetowa: www.policja.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 przeprowadzenia aukcji elektronicznej, o której mowa w art. 91a – 91e ustawy Pzp.
3. Zamawiający przewiduje przeprowadzenie postępowania w tzw. procedurze odwróconej, o której mowa w art. 24 aa ust 1 ustawy Pzp.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management).

   Szczegółowy opis przedmiotu zamówienia został zawarty w Załączniku nr 2 do SIWZ.
2. Przedmiot zamówienia określony został we Wspólnym Słowniku Zamówień:
   CPV: 48730000-4, 48821000-9.
3. Zamawiający nie dopuszcza składania ofert częściowych.
4. Zamawiający nie dopuszcza oraz nie wymaga składania ofert wariantowych.
5. Zamawiający nie przewiduje możliwości udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt. 6 i 7 lub art. 134 ust. 6 pkt 3 ustawy Pzp.
6. Zamawiający dopuszcza powierzenie zamówienia podwykonawcom Wykonawcy.
7. Wykonawca ma obowiązek (zgodnie z art. 36 b ust. 1 ustawy Pzp) wskazania w ofercie części zamówienia, których zamierza powierzyć podwykonawcom, **i podania firm podwykonawców.** Brak powyższej informacji w ofercie oznaczać będzie, że Wykonawca nie będzie korzystał z podwykonawstwa przy realizacji zamówienia.
8. 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, który powołuje się na rozwiązania równoważne opisywanym przez zamawiającego, jest obowiązany wykazać w złożonej ofercie, że oferowane przez niego dostawy, spełniają wymagania określone przez zamawiającego.
9. W nawiązaniu do art. 30 ust. 4 ustawy Pzp, jeżeli Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 30 ust. 1 pkt 2 i ust. 3, Zamawiający dopuszcza rozwiązania równoważne opisywanym. Ponadto, należy przyjąć, że wszystkim takim odniesieniom towarzyszą wyrazy „lub równoważne". Za równoważną zostanie uznana norma potwierdzająca spełnienie minimalnych parametrów określonych w normie wymaganej przez Zamawiającego. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego w zakresie norm, jest obowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego.
10. 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 końcowy realizacji zamówienia: **nie później niż do dnia 17 grudnia 2018 r.**

VI. WARUNKI UBIEGANIA SIĘ O UDZIELENIE ZAMÓWIENIA:

O zamówienie może się ubiegać Wykonawca, który:

1. spełnia następujące warunki udziału w postępowaniu, dotyczące:
   1) **zdolności technicznej lub zawodowej, w tym:**

      wykonanie w okresie trzech lat przed terminem składania ofert, a jeżeli okres prowadzenia działalności jest krótszy, to w tym okresie, co najmniej 2 dostaw i wdrożenia oprogramowania w zakresie systemów bezpieczeństwa teleinformatycznego o wartości min. 500.000 zł brutto każda.

2. Nie podlega wykluczeniu z postępowania na podstawie art. 24 ust. 1 i 5 ustawy Pzp.

   Zgodnie z art. 24 ust. 5 ustawy Pzp Zamawiający wykluczy Wykonawcę:

   1) w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2017 r. poz. 1508 tj.) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust.1 ustawy z dnia 28 lutego 2003 r.– Prawo upadłościowe (Dz.U. z 2017 r. poz.2344 tj)
   2) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;
   3) jeżeli Wykonawca lub osoby, o których mowa w ust. 1 pkt 14, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 z:
      a) Zamawiającym,
      b) osobami uprawnionymi do reprezentowania Zamawiającego,
      c) członkami komisji przetargowej,
      d) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a
         – chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu;
   4) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z Zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;
   5) będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3000 złotych;

6) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie, o którym mowa w pkt 5;
7) wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3000 złotych;
8) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w ust. 1 pkt 15, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

3. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.
4. Zamawiający może, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.
5. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20 lub ust. 5 ustawy Pzp, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu Wykonawcy. Przepisu zdania pierwszego nie stosuje się, jeżeli wobec Wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.
6. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu Wykonawcy, uzna za wystarczające dowody przedstawione na podstawie art. 24 ust. 8 ustawy Pzp.
7. W przypadkach, o których mowa w art. 24 ust. 1 pkt 19 ustawy Pzp, przed wykluczeniem Wykonawcy, Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji. Zamawiający wskazuje w protokole sposób zapewnienia konkurencji.

VII. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY

Zgodnie z przepisami ustawy Pzp oraz Rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. *w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia publicznego* (Dz. U. 2016, poz. 1126):

1. **W celu wykazania spełniania warunków, o których mowa w Rozdz. VI ust. 1 SIWZ oraz braku podstaw wykluczenia Zamawiający żąda złożenia wraz z ofertą następujących dokumentów:**
   1.1. Oświadczenie stanowiące wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu w formie Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ).
   Na potwierdzenie spełnienia warunków udziału Zamawiający wymaga wypełnienia jedynie sekcji α Cześć IV: *Kryteria kwalifikacji* JEDZ.
   W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, Jednolity Europejski Dokument Zamówienia składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu lub kryteriów selekcji oraz brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu lub kryteriów selekcji oraz brak podstaw wykluczenia.
   1.2. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu: składa Jednolity Europejski Dokument Zamówienia dotyczący podwykonawców.

UWAGA!

1. JEDZ należy przesłać w postaci elektronicznej **opatrzonej kwalifikowanym podpisem elektronicznym**. Oświadczenia podmiotów składających ofertę wspólnie oraz podmiotów udostępniających potencjał składane na formularzu JEDZ **muszą** mieć formę dokumentu elektronicznego, podpisanego kwalifikowanym podpisem elektronicznym przez każdego z nich w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 22 ust. 1 ustawy Pzp. Analogiczny wymóg dotyczy JEDZ składanego przez podwykonawcę, na podstawie art. 25a ust. 5 pkt 1 ustawy Pzp.
2. Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez wykonawcę, jest poczta elektroniczna.
   UWAGA! Złożenie JEDZ wraz z ofertą **w innej formie, w tym np.** na nośniku danych (np. CD, pendrive) jest niedopuszczalne, nie stanowi bowiem jego złożenia przy użyciu środków komunikacji elektronicznej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 o świadczeniu usług drogą elektroniczną (Dz. U. 2002, nr 144, poz. 1204 z późn. zm.)
   JEDZ należy przesłać na adres email: zamowieniakgp@policja.gov.pl
   a) Zamawiający dopuszcza w szczególności następujący format przesyłanych danych: .pdf, .doc, .docx, odt.

b) Wykonawca wypełnia JEDZ, tworząc dokument elektroniczny. Może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu elektronicznego, w szczególności w jednym z ww. formatów.

c) Po stworzeniu lub wygenerowaniu przez wykonawcę dokumentu elektronicznego JEDZ, wykonawca podpisuje ww. dokument kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w ustawie.

d) Podpisany dokument elektroniczny JEDZ **musi** zostać zaszyfrowany, tj. opatrzony hasłem dostępowym, którego podanie będzie wymagane do otwarcia dokumentu. W tym celu wykonawca może posłużyć się narzędziami oferowanymi przez oprogramowanie, w którym przygotowuje dokument oświadczenia (np. Adobe Acrobat).

e) Wykonawca zamieszcza hasło dostępu do pliku JEDZ w treści swojej oferty, składanej formie pisemnej.

f) Wykonawca przesyła zamawiającemu zabezpieczony i podpisany kwalifikowanym podpisem elektronicznym JEDZ na wskazany adres poczty elektronicznej w taki sposób, aby dokument ten dotarł do zamawiającego przed upływem terminu składania ofert. W temacie i treści przesłanej wiadomości należy wskazać oznaczenie i nazwę postępowania, którego JEDZ dotyczy oraz nazwę wykonawcy, np. JEDZ_sprawa_nr_....._nazwa_wykonawcy)

g) Wykonawca, przesyłając JEDZ, żąda potwierdzenia dostarczenia wiadomości zawierającej JEDZ.

h) Datą przesłania JEDZ będzie potwierdzenie dostarczenia wiadomości zawierającej JEDZ z serwera pocztowego zamawiającego.

i) Powyższe wymagania, z wyłączeniem obowiązku **zabezpieczenia hasłem** dotyczą również JEDZ składanego w postaci elektronicznej w odpowiedzi na wezwanie z art. 26. ust. 3 ustawy Pzp.

2. W celu wykazania, że oferowane dostawy spełniają wymagania Wykonawca składa wraz z ofertą:

2.1 W przypadku zaoferowania rozwiązania równoważnego, opis rozwiązania potwierdzający szczegółowo spełnienie wymagań określonych w *Opisie przedmiotu zamówienia* (Załącznik 2 do SIWZ).

2.2 Wydruk testów wydajnościowych dla procesorów CPU Benchmarks, zgodnie z wymogami określonymi w *Opisie przedmiotu zamówienia* (Załącznik 2 do SIWZ), punkty 19 i 20.

3. Ponadto Wykonawca musi złożyć:

3.1. Wypełniony Formularz ofertowy (o treści zgodnej z załącznikiem nr 1 do SIWZ).

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

4. Korzystanie z zasobów podmiotów trzecich

4.1. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.

4.2. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

4.3. Zamawiający ocenia, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 i ust. 5 ustawy Pzp.

4.4. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.

4.5. Wykonawca, który polega na sytuacji finansowej lub ekonomicznej innych podmiotów, odpowiada solidarnie z podmiotem, który zobowiązał się do udostępnienia zasobów, za szkodę poniesioną przez Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.

4.6. **Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu lub kryteriów selekcji składa Jednolite Europejskie Dokumenty Zamówienia dotyczący tych podmiotów.**

4.7. W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy Pzp, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący Wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający **żąda złożenia wraz z ofertą** dokumentów, które określają w szczególności:

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

Wykonawca powołujący się na zasoby podmiotu trzeciego musi złożyć wraz z ofertą pisemne zobowiązanie podmiotu trzeciego (w formie oryginału) do oddania do dyspozycji Wykonawcy niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia oraz dowody, że osoba podpisująca takie zobowiązanie, była uprawniona do działania w imieniu podmiotu trzeciego. Pełnomocnictwo należy składać formie oryginału lub kopii poświadczonej notarialnie za zgodność z oryginałem.

5. **Zamawiający, w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 oraz informacji zawartych w Jednolitym Europejskim Dokumencie Zamówienia (Wykonawców, podwykonawców, podmiotów trzecich), będzie żądał złożenia następujących aktualnych dokumentów:**

5.1 W celu wykazania spełnienia warunków udziału w postępowaniu:

5.1.1 wykazu dostaw wykonanych, potwierdzającego spełnianie warunku określonego w Rozdziale VI ust. 1 pkt. 1) SIWZ, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy lub usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy;

w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu;

5.2 W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia:

5.2.1 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 na podstawie art. 24 ust. 5 pkt 1 ustawy Pzp.

5.2.2 zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

5.2.3 zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo

wniosków o dopuszczenie do udziału w postępowaniu, lub innego dokumentu potwierdzającego, że Wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

5.2.4 informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy Pzp oraz, odnośnie skazania za wykroczenie na karę aresztu, w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt 5 i 6 ustawy Pzp, wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu.

5.2.5 oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo - w przypadku wydania takiego wyroku lub decyzji - dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności.

5.2.6 oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne.

5.2.7 oświadczenia Wykonawcy o braku wydania prawomocnego wyroku sądu skazującego za wykroczenie na karę ograniczenia wolności lub grzywny w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt 5 i 6 ustawy Pzp.

5.2.8 oświadczenia Wykonawcy o braku wydania wobec niego ostatecznej decyzji administracyjnej o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym w zakresie określonym przez Zamawiającego na podstawie art. 24 ust. 5 pkt 7 ustawy Pzp.

5.2.9 oświadczenia Wykonawcy o niezaleganiu z opłacaniem podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz. U. z 217 r. poz. 1785 tj.).

6. Wykonawca mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej:

6.1. zamiast dokumentów wymienionych w pkt. 5.2.4, składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 oraz ust. 5 pkt 5 i 6 ustawy Pzp;

6.2. zamiast dokumentu wymienionego w pkt. 5.2.1, 5.2.2, 5.2.3, składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:

a) nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał

przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,

b) nie otwarto jego likwidacji ani nie ogłoszono upadłości

Dokumenty, o których mowa w ust. 6.1 i ust. 6.2 lit. b, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu. Dokument, o którym mowa w ust. 6.2 lit. a, powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem tego terminu.

Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w pkt 6.1 oraz pkt 6.2, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania tej osoby. Przepis § 7 ust. 2 *Rozporządzenia w sprawie rodzajów dokumentów* stosuje się.

W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów odpowiednio kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w pkt. 5.2.4, składa dokument, o którym mowa w pkt 6.1 w zakresie określonym w art. 24 ust. 1 pkt 14 i 21 oraz ust. 5 pkt 6 ustawy Pzp. Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Przepis § 7 ust. 2 zdanie pierwsze *Rozporządzenia w sprawie rodzajów dokumentów* stosuje się. W przypadku wątpliwości co do treści dokumentu złożonego przez Wykonawcę, Zamawiający może zwrócić się do właściwych organów kraju, w którym miejsce zamieszkania ma osoba, której dokument dotyczy, o udzielenie niezbędnych informacji dotyczących tego dokumentu.

7. Wymagana forma składanych dokumentów:

7.1. Oświadczenia, o których mowa w rozporządzeniu dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22a ustawy Pzp oraz dotyczące podwykonawców, składane są w oryginale.

7.2. Dokumenty, o których mowa w rozporządzeniu, inne niż oświadczenia, o których mowa w ust. 1, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem.

7.3. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.

7.4. 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.

7.5. 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.

7.6. Poświadczenie za zgodność z oryginałem winno być sporządzone w sposób umożliwiający identyfikację podpisu,

7.7. Dokumenty sporządzone w języku obcym należy złożyć wraz z ich tłumaczeniem na język polski.

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

1. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami jest Andrzej Kuczyński - Wydział Zamówień Publicznych i Funduszy Pomocowych Biura Finansów KGP, tel. (22) 60 122-47.
2. Zamawiający urzęduje w dniach od poniedziałku do piątku w godz. od 8.15 do 16.15 (z wyłączeniem 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 po godzinach urzędowania (tj., która wpłynie do Zamawiającego po godzinie 16:15) zostanie zarejestrowana w następnym dniu pracy Zamawiającego.
5. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia. Zamawiający niezwłocznie udzieli wyjaśnień, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął po upływie terminu składania wniosku, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o udzielenie wyjaśnień treści SIWZ.

IX. WYMAGANIA DOTYCZĄCE WADIUM:

1. Przystępując do przetargu, Wykonawca zobowiązany jest wnieść wadium, zaznaczając cel wpłaty, w wysokości: 90.000,00 zł (słownie: dziewięćdziesiąt 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. z 2018 r., poz. 110 t.j.).
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 wadium - nr sprawy 189/BŁiI/18/AK/PMP**

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 z wyłączeniem dni ustawowo wolnych od pracy, 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 Pzp na każde pisemne żądanie zgłoszone przez Zamawiającego w terminie związania ofertą.
7. Oferta Wykonawcy, która nie będzie zabezpieczona wadium w wymaganej formie zostanie odrzucona.
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 i 3a, z przyczyn leżących po jego stronie, nie złożył oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1, oświadczenia, o którym mowa w art. 25a ust. 1, pełnomocnictw lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3, co spowodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej.

X. TERMIN ZWIĄZANIA OFERTĄ:

Termin związania ofertą wynosi 60 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 (treść formularza stanowi załącznik nr 1 do SIWZ).
2. Wykonawca ma prawo złożyć tylko jedną ofertę.
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,
   - w odniesieniu do wymogów określonych w art. 22 ust.1 ustawy Pzp Zamawiający będzie brał pod uwagę łączny potencjał techniczny, kadrowy, kwalifikacje, wiedzę i doświadczenie Wykonawców, a także ich łączną sytuację ekonomiczną i finansową,
   - 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. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 ustawy Pzp protokół postępowania jest jawny, z zastrzeżeniem art. 8 ust. 3 i 4 ustawy Pzp.
9. Wykonawcy ponoszą wszelkie koszty związane z przygotowaniem i złożeniem oferty. Wykonawcy zobowiązują się nie podnosić jakichkolwiek roszczeń z tego tytułu względem Zamawiającego.
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:

1. <u>Miejsce i termin składania ofert:</u>

1) Ofertę wraz ze wszystkimi wymaganymi oświadczeniami i dokumentami, należy umieścić w zamkniętej kopercie, zapieczętowanej w sposób gwarantujący zachowanie poufności jej treści oraz zabezpieczającej jej nienaruszalność do terminu otwarcia ofert.
2) Koperta powinna być zaadresowana w następujący sposób:

Komenda Główna Policji, Biuro Finansów
ul. Domaniewska 36/38 02-672 Warszawa
Przetarg nr 189/BŁiI/18/AK/PMP
Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management)

Nie otwierać przed dniem 27.08 **2018 r.**

3) Koperta poza oznakowaniem jak wyżej powinna być opatrzona dokładną nazwą i adresem Wykonawcy.
4) Ofertę należy złożyć do **dnia** 27.08 **2018 r. do godz.** 9:30 w Biurze Finansów KGP, 02-672 Warszawa, ul. Domaniewska 36/38, pokój 435, tel. 22-601 32 04, w godz. 8.30 – 15.30 (od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy).

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 po upływie terminu przewidzianego na wniesienie odwołanie.

2. **Miejsce i tryb otwarcia ofert**

Publiczna sesja otwarcia ofert odbędzie się w siedzibie Zamawiającego w Warszawie przy ul. Domaniewskiej 36/38, **w dniu** .....27.08..... **2018 r. o godz.** .....10:00.....

3. **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. Wycofanie oferty z postępowania nastąpi poprzez złożenie pisemnego powiadomienia (oświadczenia) w kopercie opatrzonej napisem „WYCOFANIE" – według takich samych zasad, jakie obowiązują przy wprowadzaniu zmian do oferty.

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 łączną cenę oferty brutto należy rozumieć cenę w rozumieniu 17 art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (Dz. U. 2017 poz. 1830 tj.).
2. 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.
3. 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.
4. Rozliczenia pomiędzy Zamawiającym a Wykonawcą dokonywane będą w złotych polskich.

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

W odniesieniu do Wykonawców, którzy spełnią warunki udziału w postępowaniu o udzielenie zamówienia publicznego Zamawiający dokona oceny ofert nie odrzuconych na podstawie poniższych kryteriów.

Kryteria oceny ofert i ich znaczenie.

Lp.	Nazwa Kryterium	Waga	Współczynnik do wyznaczania liczby punktów uzyskanych przez Wykonawcę	Sposób oceny
1.	K1 – cena oferty brutto	80%	80	minimalizacja
2.	K2 – przedłużona gwarancja na sprzęt	20%	20	maksymalizacja

Sposób obliczenia punktów w odniesieniu do kryterium „K1 – cena oferty brutto:

K1 – waga 80% (maksymalnie Wykonawca może otrzymać 80 punktów)

$$K1 = \frac{\text{cena ofertowa minimalna}}{\text{cena ofertowa badana}} \times 80$$

Sposób obliczenia punktów w odniesieniu do kryterium „K2 – przedłużona gwarancja na sprzęt":

K2 – waga 20% (maksymalnie Wykonawca może otrzymać 20 punktów)

Zamawiający dla kryterium *przedłużony okres gwarancji na sprzęt* przyzna punkty według następujących zasad:

- ✓ 36 miesięcy: 0 pkt.
- ✓ 42 miesiące: 10 pkt.
- ✓ 48 miesięcy i więcej: 20 pkt.

UWAGA:

- **Zamawiający wymaga podania *przedłużonego okresu gwarancji* w pełnych miesiącach.**
- **W przypadku, gdy Wykonawca w formularzu ofertowym nie wpisze żadnego okresu gwarancji Zamawiający przyjmie, że Wykonawca oferuje minimalny okres gwarancji, tj. 36 miesiące i przyzna 0 punktów.**

- **W przypadku, gdy Wykonawca w formularzu ofertowym wpisze okres gwarancji w wymiarze poniżej 36 miesięcy Zamawiający odrzuci ofertę Wykonawcy jako niezgodną z SIWZ.**
- **W przypadku, gdy Wykonawca w formularzu ofertowym wpisze okres gwarancji w niepełnych miesiącach, Zamawiający zaokrągli podaną wartość „w dół" do pełnych miesięcy.**

Zasady wyboru oferty i udzielenia zamówienia:

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie Pzp i SIWZ oraz łącznie uzyska najwyższą liczbę punktów:
K – łączna ilość punktów uzyskana w poszczególnych kryteriach

K = K1 + K2

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

1. Zamawiający nie przewiduje dokonania wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

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. z 2017 r., poz. 1577 tj.), 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.

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 brutto zamówienia.
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,
   - w 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. 2018 poz. 110 t.j.).
3. 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).
4. 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. 3-10 ustawy Pzp.
5. Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy w sposób określony w Projekcie umowy stanowiącym załącznik nr 3 do niniejszej SIWZ.
6. W przypadku wnoszenia zabezpieczenia należytego wykonania umowy w formie gwarancji, treść gwarancji podlega, przed podpisaniem umowy, zaopiniowaniu pod względem formalno-prawnym, przez radcę prawnego KGP, kontakt poprzez osobę uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami wskazaną w rozdziale VIII niniejszej SIWZ.

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

1. Umowa na wykonanie zamówienia zostanie zawarta na warunkach określonych w Projekcie umowy – Załącznik nr 3 do SIWZ.
2. Strony przewidują możliwość dokonywania zmian w treści umowy w stosunku do treści oferty Wykonawcy w sytuacjach określonych w Projekcie umowy.

XIX. 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 10 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia.
4. Odwołanie wobec treści ogłoszenia o zamówieniu oraz wobec postanowień SIWZ wnosi się w terminie 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub SIWZ na stronie internetowej.
5. Odwołanie wobec czynności innych niż określone w pkt. 3 i 4 wnosi się w terminie 10 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 lub w postaci elektronicznej, podpisane bezpiecznym podpisem elektronicznym weryfikowanych przy pomocy ważnego kwalifikowanego certyfikatu lub równoważnego środka, spełniającego wymagania dla tego rodzaju podpisu.
7. Na orzeczenie Krajowej Izby Odwoławczej stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu.

Załączniki do specyfikacji istotnych warunków zamówienia, stanowiące jej integralną część:

Załącznik nr 1 – Formularz ofertowy.

Załącznik nr 2 – Opis przedmiotu zamówienia

Załącznik nr 3 – Projekt umowy.

Załącznik nr 4 – Wzór oświadczenia Wykonawcy o przynależności do grupy kapitałowej.

Załącznik nr 5 – Informacja dotycząca przetwarzania danych osobowych.

Załącznik nr 1 do SIWZ

spr. nr 189/BŁiI/18/AK/PMP

(pieczęć Wykonawcy)

FORMULARZ OFERTOWY

do przetargu 189/BŁiI/18/AK/PMP

1. Dane dotyczące Wykonawcy:

- Pełna nazwa
- .....

  .....
- Wykonawca jest: ☐ mikroprzedsiębiorcą/ ☐ małym przedsiębiorcą/ ☐ średnim przedsiębiorcą *(zaznaczyć właściwe)*
- Adres:

  .....

  .....
- nr telefonu:.....
- nr faksu: .....
- adres e-mail: .....
- nr konta bankowego, na które dokonywany będzie zwrot wadium:

  .....
- **hasło dostępowe do podpisanego dokumentu elektronicznego JEDZ**

  .....

My niżej podpisani, oświadczamy, iż w odpowiedzi na ogłoszenie o przetargu nieograniczonym pn. ***Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management), numer postępowania 189/BŁiI/18/AK/PMP*** składam(y) niniejszą ofertę.

2. Oświadczamy, że zapoznaliśmy się z dokumentacją przetargową udostępnioną przez Zamawiającego i nie wnosimy do niej żadnych zastrzeżeń oraz, że zamówienie będzie realizowane zgodnie z wszystkimi wymaganiami Zamawiającego określonymi w Specyfikacji Istotnych Warunków Zamówienia oraz jej załącznikach, zwaną dalej SIWZ.

3. **Oferujemy wykonanie przedmiotowego zamówienia za:**

   cenę oferty brutto - ..... zł

   (słownie:.....

   ....)

   VAT .....%

4. Oferujemy dostawę przedmiotu zamówienia spełniającego wymagania określone w Opisie Przedmiotu Zamówienia (Załącznik nr 2 do SIWZ).
5. Oferujemy okres gwarancji na dostarczony sprzęt: ..... miesięcy.
6. Potwierdzamy wykonanie przedmiotu zamówienia w terminie wskazanym w Rozdziale V SIWZ.
7. Przyjmujemy zasady płatności określone w Projekcie umowy stanowiącym Załącznik nr 3 do SIWZ.
8. Oświadczamy, że zamówienie zamierzam powierzyć **<u>następującym podwykonawcom</u>**:

   .....

   .....
9. Oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO** wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu***.
10. Uważamy się za związanych niniejszą ofertą przez okres 60 dni od upływu terminu składania ofert.
11. W razie wybrania naszej oferty zobowiązujemy się do zawarcia umowy na warunkach zawartych w SIWZ oraz miejscu i terminie określonym przez Zamawiającego;
12. Załącznikami do niniejszego formularza stanowiącymi integralną część oferty są:

1) .....

2) .....

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

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

* niepotrzebne skreślić.

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

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

Załącznik nr 2 do SIWZ

spr. nr 189/BŁiI/18/AK/PMP

OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management) wraz ze wsparciem technicznym producenta.

Rozbudowa dotyczy posiadanego przez Zamawiającego systemu SIEM – IBM QRadar o odrębną instancję wg zestawienia:

Dostarczenie przez Wykonawcę Zamawiającemu licencji, sprzętu, dokumentacji oraz realizacja warsztatów instruktażowych w zakresie przygotowania do obsługi dostarczanego przedmiotu zamówienia:

1. QRadar Software Install License + SW Subscription & Support 36 Months (D1RNCLL) – szt. 1,
2. QRadar xx29 Appliance Appliance Install Appliance + Subscription and Support 36 Months (D1RADLL) – szt. 2,
3. QRadar xx29 Appliance Appliance Install Initial Appliance Business Critical Service Upgrade 36 Months (D1RANLL) – szt. 2,
4. QRadar xx29 Appliance Appliance Install Initial Appliance Hard Drive Retention Service Upgrade 36 Months (D1RAPLL) – szt. 2,
5. QRadar Event Capacity 2.5K Events Per Second License + SW Subscription & Support 36 Months (D1RP3LL) – szt. 6,
6. QRadar Flows Capacity 10K Flows Per Minute License + SW Subscription & Support 36 Months (D1RQALL) – szt. 1,
7. QRadar Flows Capacity 25K Flows Per Minute License + SW Subscription & Support 36 Months (D1RQGLL) – szt. 1,
8. QRadar Flows Capacity 100K Flows Per Minute License + SW Subscription & Support 36 Months (D1RQTLL) – szt. 1,
9. Security QRadar Vulnerability Manager Software 60XX Install License + SW Subscription & Support 36 Months (D10VDLL) – szt. 1,
10. Security QRadar Vulnerability Manager Capacity Increase 256 Install License + SW Subscription & Support 36 Months (D10VJLL) – szt. 1,
11. QRadar Data Store Connection License + SW Subscription & Support 36 Months (D1VRWLL) – szt. 2,
12. QRadar Network Insights Appliance Install Appliance + Subscription and Support 36 Months (D1PZCLL) – szt. 1,
13. QRadar Network Insights Appliance per Appliance Install Initial Appliance Business Critical Service Upgrade 36 Months (D1PZELL) – szt. 1,
14. QRadar Network Insights Appliance per Appliance Install Initial Appliance Hard Drive Retention Service Upgrade 36 Months (D1PZFLL) – szt. 1,
15. QRadar High Availability Software Install License + SW Subscription & Support 36 Months (D1RS0LL) – szt. 2,
16. QRadar xx29 Appliance Appliance Install Appliance + Subscription and Support 36 Months (D1RADLL) – szt. 2,

17. QRadar xx29 Appliance Appliance Install Initial Appliance Business Critical Service Upgrade 36 Months (D1RANLL) – szt. 2,
18. QRadar xx29 Appliance Appliance Install Initial Appliance Hard Drive Retention Service Upgrade 36 Months (D1RAPLL) – szt. 2,
19. Appliance SIEM typu 1 – szt. 1 w ukompletowaniu min.:
    a) Procesor: 2szt o poniższej specyfikacji:
        - liczba rdzeni: 14;
        - liczba wątków: 28;
        - bazowa częstotliwość: 2,40 GHz;
        - maks. Częstotliwość: 3,30 GHz;
        - cache: 35 MB;
        - Szybkość magistrali: 9.6 GT/s QPI;
        - Liczba linków QPI: 2;
        - TDP: 120 W;
        - Warunki użytkowania: Server/Enterprise;
    b) interfejsy sieciowe: dwa adaptery NT40E3 4P 40G z czterema interfejsami 10 Gbps SFP+ SR, cztery interfejsy 10/100/1000 Base-T zarządzania, jeden interfejs 10/100/1000 Base-T zdalnego zarządzania appliance,
    c) pamięć: 128 GB, 8 x16 GB truDDR4 2133MHz Memory,
    d) dysk: 2 x 200 GB SSD (RAID 1),
    e) zasilanie: dwa zasilacze 900 W AC
20. Appliance SIEM typu 2 – szt. 4 w ukompletowaniu min.:
    a) procesor: 2 szt. o poniższej specyfikacji:
        - liczba rdzeni: 12;
        - liczba wątków: 24;
        - bazowa częstotliwość: 2,20 GHz;
        - maks. Częstotliwość: 2,90 GHz;
        - cache: 30 MB SmartCache;
        - szybkość magistrali: 9,6 GT/s QPI;
        - liczba linków QPI: 2;
        - TDP: 105 W;
    b) interfejsy sieciowe: X520 2P 10GbE + 2x 10G SR, 8Gb FC 2P HBA + x2 8G, cztery interfejsy 10/100/1000 Base-T Ethernet interfaces, jeden interfejs 10/100 Base-T zdalnego zarządzania appliance,
    c) pamięć: 128 GB, 8 x 16 GB 2400 MHz DDR4 RDIMM,
    d) dysk: 12 x 3.5 inch 6 TB SAS 7.2 K rpm, 72 TB total,
    e) zasilanie: dwa zasilacze 900 W AC

lub równoważnego rozwiązania spełniającego następujące wymagania:

1) System musi zostać dostarczony w formie kompletnego rozwiązania na które składają się moduły sprzętowe (appliance) oraz moduły programowe (licencje),
2) Pełna zgodność i kompatybilność z posiadanym przez Zamawiającego systemem SIEM IBM QRadar,
3) Rozwiązanie musi umożliwiać wdrożenie pełnej wymaganej funkcjonalności tylko z użyciem wersji typu appliance,
4) System musi zapewniać obsługę i wydajność na poziomie minimum 15 000 zdarzeń na sekundę (EPS, Events per Second) oraz 150 000 przepływów na minutę (Flow per Minute),

5) System musi umożliwiać integrację z innymi rozwiązaniami bezpieczeństwa (network intelligence, incident forensic, risk management, etc.) do czego niezbędne są następujące mechanizmy:
   a) zdolność do przekazywania dalej logów i danych o aktywności sieciowej z SIEM do innych rozwiązań;
   b) zdolność do zbierania logów z dowolnych produktów bezpieczeństwa, w celu ich przechowywania, normalizacji i analizy,
   c) zdolność do integracji z rozwiązaniami potrafiącymi dokonać rejestracji pakietów sieciowych powiązanych z zarejestrowanymi zdarzeniami (np. urządzenia IPS), wraz z możliwością przekazywania dalej zgromadzonych danych,
   d) zdolność adaptacji/rekonfiguracji/przystosowania SIEM do współpracy z różnymi rozwiązaniami bezpieczeństwa poprzez edycję ustawień i/lub skrypty,
   e) zdolność do przekazania dalej skorelowanej informacji o wykrytym ataku lub działaniu niepożądanym do innych rozwiązań bezpieczeństwa i/lub urządzeń sieciowych,
6) Rozwiązanie musi umożliwiać dostosowanie systemu do indywidualnych potrzeb Zamawiającego, szczególnie w zakresie:
   a) możliwości edycji i dowolnego konfigurowania widoków danych bezpieczeństwa na pulpitach (dashboards),
   b) możliwości edycji, dowolnego konfigurowania i tworzenia nowych reguł korelacji zdarzeń, tak aby możliwym było dopasowanie działania do konkretnych przypadków użycia, zarządzania ryzykiem, monitorowania zgodności z wytycznymi i przepisami,
   c) możliwość edycji, dowolnego konfigurowania i tworzenia nowych szablonów raportów,
   d) możliwość tworzenia, konfigurowania i zapisywania zapytań, wyszukiwań, widoków wykorzystywanych przy analizie, w celu późniejszej analizy lub ponownego wykorzystania raz użytych składni i założeń,
7) Rozwiązanie musi zapewniać elastyczną skalowalność, tak w zakresie rozbudowy wydajnościowej pod kątem zwiększenia liczby obsługiwanych zdarzeń (EPS) czy terminu i liczby ich składowania, jak również pod kątem rozbudowy geograficznej systemu, poprzez wyniesione moduły agregacji i retencji danych (zdarzenia, przepływy sieciowe, etc.), zdalne dostępy do konsoli na różnym poziomie dostępu, przy jednoczesnym zachowaniu centralnego: zarządzania, korelacji, zależności czy zakresie wyszukiwania i raportowania. Wymaganie w zakresie zbierania danych dotyczy mechanizmów agentowych i bez-agentowych,
8) Rozwiązanie musi obsługiwać rozproszone źródła danych (zdarzenia, aktywność sieciowa) w taki sposób, aby wszystkie zebrane dane były dostępne z jednego interfejsu użytkownika,
9) Rozwiązanie musi zapewniać integralność zebranych informacji, chroniąc zgromadzone i przetwarzane dane źródłowe przed manipulacją i utratą,
10) Rozwiązanie musi umożliwiać rozproszoną korelację zdarzeń, tzn. musi potrafić skorelować np. wielowątkowe zdarzenia z różną liczbą zdarzeń z różnych źródeł i mechanizmów zbierania danych. Dane podlegające globalnej korelacji mogą pochodzić zarówno z dowolnych modułów zbierania danych (collectors) jak i wyników innych mechanizmów korelacyjnych. Pożądaną funkcjonalnością jest możliwość zastosowania zbudowanej reguły korelacji globalnie i lokalnie,

11) Rozwiązanie musi umożliwiać tagowanie/klasyfikowanie zdarzeń, w celu późniejszego szybszego wyszukiwania, korelacji, raportowania. Mechanizm tagowania/klasyfikacji prócz wbudowanych zasad, musi umożliwiać ustalanie własnych zasad użytkownika systemu,
12) Rozwiązanie musi zapewniać przejrzystość w zakresie realizowanych funkcji zbierania, agregacji, sortowania, filtrowania czy korelacji danych, we wszystkich komponentach, również w sytuacji ich geograficznego lub modułowego rozproszenia,
13) Rozwiązanie powinno umożliwiać wielowątkowość w zakresie obsługi różnych domen/ środowisk (różnych obsługiwanych systemów/klientów przez jedna instancję SIEM), w których mogą wystąpić takie same adresy IP, nazwy hostów, etc. np,: poprzez odpowiednie tagowanie lub oznaczanie pochodzenia zgromadzonych zdarzeń, wraz z zachowaniem możliwości ich niezależnego(one domain) lub całościowego (cross domain) korelowania w systemie,
14) Rozwiązanie musi wspierać mechanizm „master console" (jedna konsola dla wielu instancji SIEM),
15) Rozwiązanie musi umożliwiać centralne zarządzanie wszystkimi komponentami systemu oraz wszystkimi funkcjami administracyjnymi, z jednej webowej konsoli zarządzającej,
16) Rozwiązanie musi umożliwiać takie zarządzanie uprawnieniami, aby możliwe było ograniczenie dostępu do danych dotyczących systemu i/lub konkretnego środowiska/domeny (np. poprzez ograniczenie dostępu do danych z konkretnego kolektora) dla wybranych użytkowników systemu i różnych poziomów funkcjonalności - zgodnie z modelem RBAC (ang. role-based access control, kontrola dostępu oparta na rolach),
17) Rozwiązanie musi posiadać takie mechanizmy zarządzania uprawnieniami, aby możliwe było przez administratora stworzenie i definiowanie ról/grup/użytkowników z dostępem opartym o model RBAC. W szczególności chodzi o zdolność mechanizmów bezpieczeństwa systemu do indywidualnego nadawania lub ograniczania uprawnień poszczególnym użytkownikom i/lub grupom/rolom w zakresie określonych funkcji rozwiązania (administracja, raportowanie, filtrowanie zdarzeń, korelacja, podgląd pulpitów, etc.),
18) Rozwiązanie powinno posiadać mechanizm ukrywania (obfuskacji) danych, wraz z możliwością wskazania jakie dane powinny być ukrywane,
19) Rozwiązanie musi umożliwiać tworzenie niezależnych i niedostępnych dla wszystkich pulpitów z widokami dla specjalnych działań np. SOC, NOC. Takie pulpity powinny być widoczne tylko dla wybranych użytkowników i/lub ról/grup użytkowników, poprzez niezależną konsolę webową,
20) Rozwiązanie musi umożliwiać szyfrowanie komunikacji pomiędzy poszczególnymi modułami systemu i zbierania danych,
21) Rozwiązanie musi umożliwiać integrację z zewnętrznymi dostawcami mechanizmów uwierzytelniania (LDAP, AD, RADIUS, etc...) dla operatorów i administratorów systemu
22) Rozwiązanie powinno posiadać wsparcie producenta, ale też wsparcie w formie dostępnego forum wymiany wiedzy/doświadczeń dotyczące produktu, które zostanie udostępnione bez limitu operatorom i administratorom systemu.
23) System powinien umożliwiać zwiększenie możliwości operacyjnych np. poprzez dodanie dodatkowych licencji, bez potrzeby zwiększania liczby fizycznych komponentów systemu do 300 000 przepływów na minutę (Flow per Minute),
24) Rozwiązanie powinno posiadać mechanizmy usprawniające jego wykorzystanie i wdrożenie, np.:
    a) automatyczne wykrywanie źródeł logów,

b) automatyczne wykrywanie aplikacji,
c) automatyczne wykrywanie aktywów,
d) automatyczne wykrywanie podatności,
e) automatyczne wykrywanie anomalii,
f) automatyczne grupowanie aktywów,
g) predefiniowane reguły analizy i korelacji zdarzeń,
h) łatwe w użyciu mechanizmy filtrowania (również predefiniowane filtry),
i) zaawansowane funkcje analizy zabezpieczeń,
j) predefiniowane raporty,
k) priorytetyzacja wg zasobów,
l) automatyczne aktualizacje baz zagrożeń, wsparcia urządzeń, oprogramowania systemowego,

25) Rozwiązanie musi udostępniać graficzny interfejs webowy do zarządzania, analizy i raportowania. Zalecanym jest, aby interfejs nie wymagał żadnych wtyczek typu Java, Flash lub wymogu posiadania grubego klienta do obsługi rozwiązania,
26) Rozwiązanie musi posiadać własne i/lub wspierać zewnętrzne mechanizmy HA, szczególnie w zakresie mechanizmów akwizycji i przechowywania danych oraz centralnego zarządzania systemem,
27) Rozwiązanie musi zapewniać ciągłe działanie jak największej liczby komponentów, niezależnie od awarii jednego z nich. Np. w sytuacji awarii systemu centralnego lub modułu analitycznego, logi powinny być nadal zbierane,
28) Rozwiązanie musi posiadać mechanizmy umożliwiające zbieranie danych w czasie rzeczywistym,
29) Rozwiązanie musi posiadać zautomatyzowany proces wykonywania backupu i odzyskiwania konfiguracji z backupu,
30) Rozwiązanie musi posiadać automatyczny mechanizm kontroli stanu swoich komponentów (health check), wraz z informowaniem użytkownika o zauważonych problemach,
31) Rozwiązanie powinno posiadać pewną ilość przykładowych skonfigurowanych paneli (dashboards), prezentujących możliwości i mechanizmy systemu SIEM,
32) Rozwiązanie musi utrzymywać bazę wiedzy o wszystkich wykrytych w sieci aktywach. Baza danych o aktywach powinna umożliwiać edycję zebranych informacji, zapewniając jednak ochronę przed nieuprawnioną zmianą, oraz rozliczalność procesu wprowadzania zmian. Baza danych musi umożliwiać przeszukiwanie swojej zawartości. Wśród zgromadzonych danych o danym aktywie powinny być zawarte pewne informacje uzyskane przy wykrywaniu zasobów:
    a) atrybuty systemu,
    b) atrybuty sieciowe,
    c) stan,
    d) podatności/luki,
    e) lokalizacja,
    f) przynależność,
    g) inne właściwości, które użytkownik może samodzielnie zdefiniować i/lub wpisywać,
33) Rozwiązanie musi być zdolne obsłużyć nagły wzrost liczby zbieranych danych (EPS) jednocześnie zapewniając ciągłość zbierania danych, tak aby żaden przepływ sieciowy lub żadne zdarzenie nie zostało pominięte. W takiej sytuacji system musi jednocześnie zachować pełna funkcjonalność,

34) Rozwiązanie musi wspierać/obsługiwać produkty innych producentów w zakresie bezpieczeństwa,
35) Rozwiązanie musi wspierać informacje zbierane z systemów operacyjnych firmy Microsoft, zarówno wersji serwerowych, aplikacyjnych i funkcjonalnych, jak również z systemów użytkowników końcowych,
36) Rozwiązanie musi wspierać informacje zebrane z systemów opartych na środowiskach firmy Microsoft, w szczególności:
    a) Microsoft Sharepoint Server,
    b) Microsoft Exchange Server,
    c) Microsoft IIS,
    d) Microsoft AD,
    e) Microsoft FS,
    f) Inne
37) Rozwiązanie musi wspierać informacje zebrane z systemów typu UNIX/Linux, zarówno w wersjach serwerowych jak i w wersjach dla użytkowników końcowych,
38) Rozwiązanie musi wspierać informacje zbierane z serwerów typu mainframe,
39) Rozwiązanie musi wspierać informacje zebrane z systemów i serwerów bazodanowych klasy enterprise, w szczególności:
    a) Oracle,
    b) DB2,
    c) Microsoft,
40) Rozwiązanie musi wspierać informacje zbierane z systemów komercyjnych (np. serwery WWW/FTP, systemy klasy ERP, SAP, Oracle, itp.),
41) Rozwiązanie musi wspierać informacje zebrane z systemów i narzędzi zabezpieczających klasy DLP (Data Leak Protection),
42) System musi umożliwiać realizację wsparcia dla danych zbieranych z systemów wytworzonych w ramach prac własnych i innych niestandardowych, realizowanych w ramach zamówień indywidualnych. Aby zrealizować takie wymaganie producent i system musi umożliwiać użytkownikowi końcowemu samodzielne i nieodpłatne (bez dodatkowych licencji i kosztów w tym wsparcia technicznego), budować własne parsery logów,
43) Rozwiązanie musi wspierać informacje zebrane z systemów zabezpieczeń klasy DAM (Database Activity Monitoring),
44) Możliwość wykorzystania informacji dotyczących plików - zebranych z systemów i narzędzi bezpieczeństwa klasy FIM/FAM (File Integrity/Activity Monitoring) lub poprzez rozwiązania agentowe,
45) Rozwiązanie musi wspierać informacje zebrane z systemów i narzędzi bezpieczeństwa klasy IAM (Identity and Access Management),
46) Rozwiązanie musi wspierać informacje typu: użytkownicy, grupy, zebrane z usługi katalogowej (np. AD, LDAP), poprzez interfejs integracyjny lub plik,
47) Rozwiązanie musi wspierać informacje NetFlow - czyli dane o przepływach, np.: NetFlow, J- Flow, sFlow, PCAP, itp., zebrane samodzielnie jak również za pomocą innych narzędzi,
48) System powinien zapewniać analizę warstwy 7 modelu ISO/OSI przepływów w sieci za pomocą sprzętowego appliance o specyfikacji min.:
    - procesor: 2szt o poniższej specyfikacji:
    - liczba rdzeni: 14;
    - liczba wątków: 28;
    - bazowa częstotliwość: 2,40 GHz;
    - maks. Częstotliwość: 3,30 GHz;

- cache: 35 MB;
- Szybkość magistrali: 9.6 GT/s QPI;
- Liczba linków QPI: 2;
- TDP: 120 W;
- Warunki użytkowania: Server/Enterprise;,

- interfejsy sieciowe: dwa adaptery NT40E3 4P 40G z czterema interfejsami 10 Gbps SFP+ SR, cztery interfejsy 10/100/1000 Base-T zarządzania, jeden interfejs 10/100/1000 Base-T zdalnego zarządzania appliance
- pamięć: 128 GB, 8 x16 GB truDDR4 2133MHz Memory
- dysk: 2 x 200 GB SSD (RAID 1)
- zasilanie: dwa zasilacze 900 W AC

49) System powinien zapewniać wydajność analizy przepływów w sieci: rzędu 10 Gbps w kontekście: source ip address, source port, destination ip address, destination port ip protocol, flow id, total packets, total bytes per packets, first packet time, last packet time, source DSCP, destination DSCP, VLAN Tag, application, action, password, file name, DSN query, DNS response, Recipient users, file entropy, content type, web categories, file hash, http hosts, http referrer, http response code, search arguments, http server, http user agent, http version, originating user, request URL, SMTP Hello, content subject, suspect content descriptions.
50) Rozwiązanie musi wspierać informacje zebrane z infrastruktury sieciowej (switche, routery, itp.),
51) Rozwiązanie musi wspierać informacje zebrane z wiodących skanerów podatności,
52) Rozwiązanie musi skanować i zarządzać podatnościami w kontekście aplikacji, systemów operacyjnych, urządzeń sieciowych dla co najmniej 512 *assetów*.
53) Rozwiązanie musi posiadać architekturę pozwalającą na zbieranie i archiwizację logów oraz przepływów w sieci, w podziale na dane krótkoterminowe (tzw. online, wykorzystywane w bieżących analizach) o pojemności co najmniej 96TB oraz dane długoterminowe (tzw. offline, dane archiwizowane po określnym czasie), z wewnętrzną ale konfigurowalną obsługą mechanizmu retencji danych pomiędzy obydwoma typami,
54) Rozbudowa pojemności dla danych *online* musi uwzględniać jednocześnie zwiększenie pojemności w obszarze dysków oraz wydajności przetwarzania danych,
55) Rozwiązanie musi zapewnić archiwizację nielimitowanego licencją strumienia zdarzeń uznanych za zdarzenia typu non-security (tzn. takich które nie będą podlegać procesowi korelacji),
56) Rozwiązanie musi posiadać mechanizmy umożliwiające na efektywne przechowywanie i kompresję zbieranych danych,
57) Rozwiązanie musi wspierać branżowe mechanizmy zbierania logów (np.: syslog, WMI, JDBC, SNMP, Checkpoint, itp.),
58) Rozwiązanie musi wspierać bez-agentowe zbieranie danych, w miarę możliwości w jak największej liczbie przypadków,
59) System powinien wspierać analizę logów z sytemu MS Windows,
60) Rozwiązanie musi wspierać długoterminowe zapewnienie dostępu do szczegółowych danych odnośnie zarejestrowanych i zebranych zdarzeń czy przepływów w sieci. System powinien zapewnić dostęp do takich informacje co najmniej przez okres 12 miesięcy,
61) Rozwiązanie musi normalizować informacje zawarte w zebranych zdarzeniach (usernames, IP address, hostnames, log source, device, itp.), z urządzeń i systemów różnych dostawców,

62) Rozwiązanie musi wspierać mechanizm jednolitej i wspólnej taksonomii/klasyfikacji zdarzeń,
63) Rozwiązanie musi zapewniać możliwość przechowywania zarówno znormalizowanych danych o zdarzeniach, jak również źródłowego/oryginalnego formatu danych w tzw. postaci RAW (full payload indexing), np. dla celów późniejszej analizy w innych systemach lub przeprowadzenia analizy śledczej,
64) Rozwiązanie musi umożliwiać normalizację i agregację pól w zdarzeniach, które nie są dostępne domyślnie w istniejących mechanizmach normalizacji,
65) Rozwiązanie musi obsługiwać i/lub normalizować sygnatury czasowe zdarzeń w wielu strefach czasowych,
66) Rozwiązanie musi zapewniać analizę w czasie rzeczywistym,
67) Rozwiązanie musi zapewnić długoterminową analizę zdarzeń w poszukiwaniu tendencji incydentów,
68) Rozwiązanie musi zapewnić możliwość agregowania i analizowania zdarzeń opartych na filtrze określonego użytkownika,
69) Rozwiązanie musi umożliwiać prezentację zdarzeń w trybie real-time, przy jednoczesnym zapewnieniu pełnej funkcjonalności filtrowania prezentowanych zdarzeń,
70) Rozwiązanie musi zapewnić mechanizmy alarmowania w oparciu o zaobserwowane nieprawidłowości i zmian behawioralnych w zdarzeniach sieciowych i zdarzeniach dotyczących bezpieczeństwa,
71) Rozwiązanie musi zapewniać tworzenie i utrzymywanie historii aktywności użytkowników systemu na poszczególnych zasobach zarejestrowanych w systemie (korelacja users per assets),
72) System musi zapewniać mechanizm uzupełniania informacji o użytkowniku, w kontekście którego generowane są zdarzenia, nawet gdy informacje o użytkowniku nie są zawarte w pobieranych logach,
73) Rozwiązanie musi zapewniać raportowanie dla wszystkich przedmiotów dostępnych poprzez GUI systemu (np.: pobrane dane, zanalizowane dane, zdarzenia, przepływy, podatności, zasoby, zagrożenia, itp.),
74) Rozwiązanie musi posiadać konfigurowalny silnik raportowania, tak aby możliwe było tworzenie niestandardowych raportów bez dodatkowych kosztów (licencje i wsparcie techniczne) usług ze strony producenta,
75) Rozwiązanie musi posiadać możliwość predefiniowania automatycznego generowania raportów w określonych przedziałach czasu,
76) Rozwiązanie musi zapewnić szablony do szybkiego tworzenia i dostarczania raportów na wielu poziomach szczegółowości,
77) Rozwiązanie powinno w standardzie (out-of-the-box) zawierać zestaw gotowych raportów, obejmujących kategorie: uwierzytelnianie, tożsamość, aktywność użytkowników, zgodność, konfiguracja i zarządzanie zmianą, raport zarządczy, raporty dotyczące urządzeń, zarządzanie siecią, bezpieczeństwo, monitorowanie użycia, aktywność aplikacji,
78) Rozwiązanie powinno w standardzie (out-of-the-box) zawierać zestaw raportów dotyczących przestrzegania przepisów i norm, oraz framework'ow np. NIST, COBIT, ISO, PCI DSS, FISMA,
79) W szczególności system powinien wspierać:
    a) ISO 27001,
80) Rozwiązanie musi wspierać automatyczną dystrybucję raportów,
81) Rozwiązanie musi posiadać możliwość udostępniania raportów historycznych oraz raportów na temat trendów w czasie,

82) Rozwiązanie musi posiadać możliwość scentralizowanego raportowania o podatnościach. Aby było to możliwe, system musi realizować funkcje normalizacji/ujednolicania pozyskanych informacji odnośnie podatności (np. z różnych skanerów podatności i urządzeń bezpieczeństwa sieci),
83) Rozwiązanie musi posiadać możliwość raportowania o podatnościach i zdarzenia w podziale na konkretne pojedyncze lub grupy zasobów,
84) Rozwiązanie musi zapewniać automatyczne powiadamianie/ostrzeganie o zagrożeniach zaobserwowanych w monitorowanych urządzeniach,
85) Rozwiązanie musi zapewniać możliwość korelowania informacji pomiędzy teoretycznie niezależnymi od siebie urządzeniami,
86) Rozwiązanie musi umożliwiać analizę zebranych informacji w postaci surowej (RAW), nie ograniczając się tylko do analizy danych znormalizowanych,
87) Rozwiązanie musi realizować analizę i sygnalizowanie incydentów nie tylko na zasadzie przekroczenia ustalonego progu dla zdarzeń (treshold), ale również na zasadzie analizy behawioralnej i oceny anomalii w trendzie,
88) Rozwiązanie musi generować alerty na podstawie zauważonej zmiany w sieci dotyczącej pojawienia się nowej usługi lub gdy pojawią się nowe zasoby,
89) Rozwiązanie musi umożliwiać śledzenie przemieszczania i/lub pojawiania się nowych zasobów w monitorowanej sieci, wraz z ich jednoznaczną identyfikacją (potwierdzenie, że przemieszcza się jeden lub grupa konkretnych i zidentyfikowanych zasobów), Rozwiązanie musi wspierać mechanizm priorytetyzacji (wagi) zgłaszanych alarmów i komunikatów, powstałych na podstawie wykonanej analizy i wagi zdarzeń oraz wartości zasobu. Wymaganym jest aby waga alertu zależała od kilku zmiennych, np.: rodzaj zasobu, zasób, protokół, aplikacja, reguła korelacyjna, źródło zdarzenia (kolektor/skaner podatności/analityka SIEM), itp. Ustawienie tej wagi musi być możliwe bez dodatkowych kosztów i wsparcia technicznego ze strony producenta,
90) Rozwiązanie musi wspierać różne standardy komunikacji, w celu przekazywania alertów do innych rozwiązań. Minimalnie system musi obsługiwać następujące mechanizmy: SMTP, Email, syslog,
91) Rozwiązanie musi posiadać mechanizm inteligentnego usuwania zduplikowanych wpisów o tych samych alarmach. Rozwiązanie to powinno być w pewnym zakresie konfigurowalne przez użytkownika,
92) Rozwiązanie musi posiadać mechanizm zależności alertowania (chain alerts) o zdarzeniach. Mechanizm ten musi umożliwiać automatyczne wyzwalanie innych, a zależnych od siebie alertów. Wyzwalanie takiej łańcuchowej reakcji alarmowania musi być konfigurowalne przez użytkownika, bez dodatkowych kosztów czy profesjonalnego wsparcia ze strony producenta. Mechanizm powinien mieć również funkcję ograniczania liczby wyzwalanych alertów – zależnie od wybranego trybu działania, tak aby zgłosić najwyższy wagowo alert w łańcuchu, zamiast zgłaszania wszystkich alertów jednocześnie, przy jednoczesnym zachowaniu możliwości przeglądu wszystkich alertów które wyzwoliły reakcję łańcuchową,
93) Rozwiązanie musi posiadać mechanizmy umożliwiające podejmowanie działań, po zgłoszeniu alertu. Np. wysłanie informacji do wskazanych adresatów/systemów, uruchomienie skryptu, itp.,
94) Rozwiązanie musi posiadać zdolność korelowania zdarzeń z informacjami uzyskanymi od strony trzeciej, np. z kanałów z informacjami odnośnie zagrożeń. Taka korelacja powinna być realizowana np,: według lokalizacji geograficznej, znane wrogie sieci, kanały botnetowe, itp. Mechanizm korzystający z takich kanałów z informacjami odnośnie

bezpieczeństwa, powinien posiadać mechanizmy automatycznej aktualizacji/pobierania nowych informacji,

95) Rozwiązanie musi posiadać zdolność korelowania zdarzeń z informacjami pozyskanymi ze znanych skanerów luk bezpieczeństwa, bez dodatkowych kosztów (licencji oraz profesjonalnego wsparcia ze strony producenta),
96) Rozwiązanie musi posiadać zdolność monitorowania dzienników zdarzeń pod kątem anomalii, awarii, zmian w pobranych danych. W przypadku wykrycia niezgodności lub błędu w działaniu logu lub pobieraniu zdarzeń z logu, rozwiązanie powinno wygenerować alert,
97) Rozwiązanie powinno w standardzie (out-of-the-box) zapewniać mechanizmy zdolne do wykrywania i klasyfikacji zasobów wg typu systemu, rozpoznając np.: systemy pocztowe, serwery plików, serwery bazodanowe, itp.,
98) Rozwiązanie powinno posiadać mechanizmy umożliwiające korelację dla brakującej sekwencji zdarzeń. Chodzi tu o zdolność do wykrycia faktu restartu usługi, i odróżnienia restartu od jej zatrzymania, przy alertowaniu o zdarzeniu,
99) Rozwiązanie musi umożliwiać korelację zdarzeń wraz z upływem czasu, np. system powinien potrafić wyzwolić alert, gdy określony adres IP wysłał więcej danych do jednego odbiorcy niż określony limit, w określonym czasie,
100) Rozwiązanie musi umożliwiać wykonywanie korelacji historycznych, tzn. takich, gdzie operator może ponownie uruchomić płynną i skuteczną analizę zdarzeń przeszłych. Dzięki temu możliwe będzie wykonanie tuningu danej reguły lub reguł korelacyjnych, aby w przyszłości były bardziej precyzyjne, lub przeprowadzenie analizy śledczej zdarzeń historycznych,
101) Rozwiązanie musi posiadać mechanizmy automatycznej i ciągłej aktualizacji, wraz z dostępem do źródła tych aktualizacji. Wśród aktualizowanych danych prócz samych aktualizacji systemowych powinny się również znaleźć dane o nowych zagrożeniach, podatnościach czy wykrytych szkodliwych obiektach,
102) Rozwiązanie musi posiadać mechanizm prezentacji (wyświetlania) danych o profilu ruchu dla danego zasobu lub grupy zasobów i/lub lokalizacji. Mechanizmy te powinny umożliwiać przedstawienie takich danych jak: wielkość ruchu, ilość pakietów, liczby komunikujących się hostów. Informacje te powinny być dostępne w kontekście: aplikacji, portów, protokołów, zidentyfikowanych zagrożeń w każdym punkcie monitorowanej sieci,
103) Rozwiązanie musi posiadać zdolność do automatycznego i dynamicznego uczenia się behawioralnej charakterystyki zdarzeń i jej zmian w monitorowanym środowisku,
104) Rozwiązanie musi posiadać zdolność do wykrywania ataków typu DoS (Denial of Service) oraz DDoS (Distributed Denial of Service),
105) Rozwiązanie musi posiadać zdolność do wykrywania i prezentacji podglądu aktualnego stanu ruchu sieciowego dotyczącego wykrytych zagrożeń w sieci,
106) Rozwiązanie musi posiadać zdolność profilowania ruchu sieciowego TCP i UDP,
107) Rozwiązanie musi posiadać zdolność profilowania ruchu uwzględniając logiczną strukturę sieci,
108) Rozwiązanie musi posiadać zdolność identyfikacji ruchu sieciowego pochodzącego z potencjalnie niebezpiecznych aplikacji (file sharing, per-to-peer, tor, itp.),
109) Rozwiązanie musi posiadać zdolność graficznej prezentacji profili ruchu sieciowego pod kątem szybkości transmisji,
110) Rozwiązanie musi posiadać zdolność profilowania i prezentacji informacji w określonych przedziałach czasu. Profile takie powinny być dostępne dla okresów określonych godzinami, dniami lub tygodniami,

111) Rozwiązanie musi posiadać zdolność profilowania w czasie rzeczywistym komunikacji pochodzącej lub wysyłanej w kierunku określonej obszarem geograficznym sieci publicznej (Internet),
112) Rozwiązanie musi posiadać zdolność do tworzenia skutecznych i niezależnych profili zróżnicowanych pod kątem ruchu lokalnego i ruchu pochodzącego lub wysyłanego do sieci Internet (innych sieci zewnętrznych - np. WAN, VPN),
113) Rozwiązanie musi umożliwiać użytkownikowi tworzenie własnych niezależnych profili i widoków, przy wykorzystaniu dowolnej właściwości przepływu, logów czy danych źródłowych, lub informacji z już sprofilowanego ruchu,
114) Rozwiązanie musi obsługiwać profilowanie ruchu w oparciu o pojedyncze adresy IP, grupy adresów IP, adresy źródłowe/docelowe, itp.,
115) Rozwiązanie musi zapewnić możliwość wyodrębnienia konkretnych i zdefiniowanych przez użytkownika pól/danych z przechwyconego ruchu sieciowego, a następnie umożliwić wykorzystanie tych danych w regułach korelacyjnych,
116) Rozwiązanie musi być zdolne do identyfikacji ruchu sieciowego w sieciach środowisk wirtualnych,
117) Rozwiązanie musi posiadać zdolność do kontekstowego łączenia aktywności aplikacji w sieci ze zdarzeniami bezpieczeństwa pochodzącymi z monitorowanych urządzeń/zasobów,
118) Rozwiązanie musi posiadać zdolność do kontekstowego łączenia w trybie rzeczywistym raportowanych zdarzeń bezpieczeństwa z wiedzą o poszczególnych monitorowanych zasobach, które są celami lub źródłami ataków,
119) Rozwiązanie musi zapewniać możliwość automatycznego nadawania wagi/priorytetu raportowanym zdarzeniom bezpieczeństwa, w zależności od wartości i istotności zasobu który jest celem lub źródłem ataku,
120) Rozwiązanie musi posiadać zdolność do automatycznego nadawania wagi/priorytetu przy nasilonym raportowaniu zdarzeń bezpieczeństwa, w zależności od podatności zasobu, który jest celem lub źródłem ataku,
121) Rozwiązanie musi zapewnić możliwość przypisania ocen w zakresie wiarygodności przekazywanych informacji, monitorowanym rozwiązaniom z zakresu bezpieczeństwa,
122) Rozwiązanie musi posiadać zdolność do prezentacji w czasie rzeczywistym monitorowanych zdarzeń w źródłowym (RAW) i przetworzonym/znormalizowanym formacie danych,
123) Rozwiązanie musi zapewnić mechanizm automatycznej korekty współczynników korygujących wiarygodność urządzeń bezpieczeństwa, w sytuacji reakcji na całą sieć,
124) Rozwiązanie musi posiadać zdolność do wysyłania powiadomień o alertach z wykorzystaniem dobrze znanych metod (SNMP traps, email, itp,),
125) Rozwiązanie musi posiadać mechanizmy typu workflow, pozwalające realizować działania związane z obsługą incydentu,
126) Rozwiązanie musi posiadać zdolność obustronnej komunikacji z rozwiązaniami bezpieczeństwa stron trzecich, w zakresie systemów ticketowania/heldpesk, które operatorzy systemu mogą wykorzystywać w celu realizacji swoich zadań,
127) Rozwiązanie musi zapewnić możliwość uchwycenia i prezentacji wszystkich istotnych aspektów incydentu bezpieczeństwa w jednym logicznym widoku. Widok taki powinien zawierać minimalnie informacje typu: powiązane zdarzenia, aktywność sieciowa, skorelowane alerty, skorelowane podatności w powiązanych systemach, itp.,

128) Rozwiązanie musi posiadać funkcjonalność, umożliwiającą opisanie, zapisanie i przekazanie incydentu bezpieczeństwa do innych linii wsparcia (np. od operatorów monitoringu do analityków bezpieczeństwa I i II linii),
129) Rozwiązanie musi posiadać mechanizm umożliwiający śledzenie incydentów bezpieczeństwa w kontekście różnych atrybutów (adres IP, adres MAC, nazwa użytkownika, źródło incydentu czy reguła korelacji, również na podstawie reguł zdefiniowanych przez użytkownika). Konteksty te powinny umożliwiać filtrowanie zdarzeń wg określonych parametrów,
130) Rozwiązanie powinno umożliwiać jego operacyjne wykorzystanie bez nakładu pracy programistycznej w zakresie budowy reguł korelacyjnych, scenariuszy, raportów, kokpitów roboczych,
131) Producent rozwiązania powinien dysponować Autoryzowanym Ośrodkiem Szkoleniowym (ATC) umożliwiającym przeprowadzenie certyfikowanego szkolenia. W cenie rozwiązania powinno być ujęte szkolenie dla min. 6 administratorów i operatorów systemu w zakresie rozszerzonym: instalacja rozwiązania, administracja, obsługa funkcjonalności wraz z prezentacją poszczególnych opcji interfejsu graficznego oraz szkolenia zaawansowane dla 6 administratorów, uwzględniające zaawansowaną konfigurację rozwiązania z uwzględnieniem różnych źródeł danych, zaawansowane wykorzystanie funkcjonalności systemu, w tym funkcji analitycznych, budowanie skryptów, zaawansowane administrowanie i rozwiązywanie problemów z aplikacją. Szkolenie zostanie przeprowadzone indywidualnie dla Zamawiającego w 2 edycjach po 3 osoby w grupie.
132) W cenie rozwiązania powinny znaleźć się 36-miesięczne licencje:
    a) uwzględniające rozwiązywanie problemów z oprogramowaniem w trybie min. 5x8,
    b) umożliwiające dostęp do dokumentacji produktowej i problemowej,
    c) umożliwiające dostęp do forum wymiany wiedzy/doświadczeń,
    d) umożliwiające dostęp do aktualizacji wzorców i próbek dla mechanizmów korelacyjnych i detekcyjnych,
    e) umożliwiające codzienne aktualizacje (update) dostępne dla Systemu,
    f) umożliwiające podnoszenie wersji (upgrade) produktów,
    g) umożliwiające dostęp do bazy wiedzy oraz przewodników produktowych, poprawek, aktualizacji i nowych wersji oprogramowania w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego Oprogramowania,
133) Rozwiązanie ma obejmować swoim funkcjonowaniem dwie różne lokalizacje pracujące w trybie active-active,
134) Licencje powinny być bezterminowe i nieuzależnione od wykupienia lub przedłużenia wsparcia producenta,
135) Wykonawca gwarantuje, że rozwiązanie będzie wspierane przez co najmniej 5 lat, i w tym czasie nie nastąpi wstrzymanie wsparcia dla zakupionego produktu (EoL – End of Life, EoS – End of Support),
136) System powinien być wyposażony w funkcjonalność lub odrębne rozwiązanie dostarczające mechanizmy prowadzenia dochodzeń i przebiegu incydentu po jego wykryciu,
137) W przypadku, gdy funkcjonalność dochodzeń dostarczona będzie jako odrębne narzędzie, powinno być ono zintegrowane z systemem analiz i korelacji zdarzeń na poziomie danych (korzystanie z danych zgromadzonych w systemie) oraz interfejsu użytkownika (jako minimum uruchomienie mechanizmów dochodzeń z konsoli systemu analiz i korelacji zdarzeń),

138) Mechanizm analizy przebiegu incydentu powinien wykorzystywać zgromadzone dane, uwzględniające zdarzenia w logach, przepływy netflow, a także pełne zrzuty danych pakietowych oraz dane zgromadzone w plikach. System powinien umożliwiać analizy danych dostępnych na Twitterze, Facebooku, wynikach wyszukiwania, dokumentach wytwarzanych przez aplikacje, pakietach VoIP (w tym możliwość odtworzenia konwersacji),
139) Możliwość analizy na poziomie sieciowym, kto był zaangażowany w incydent, co się stało, kiedy zaszło zdarzenie, jakie dane zostały udostępnione lub przekazane,
140) Możliwość wyszukiwania malware'u i aktywności związanych z jego działaniem,
141) System zapewnia rekonstrukcję surowych danych sieciowych związanych z incydentem bezpieczeństwa,
142) System zapewnia możliwości wielowymiarowej analizy danych sieciowych celem zidentyfikowania relacji między obiektami (zasobami, osobami) zaangażowanymi w incydent,
143) System analizuje dane z uwzględnieniem wszystkich danych sieciowych, pakietów, metadanych, treści, w tym tekst stron internetowych, dokumenty i elementy bazy danych,
144) System posiada możliwości filtrowania wyników wyszukiwania celem wykrycia wyłącznie pakietów związanych z danym incydentem,
145) System umożliwia weryfikację obserwowanego wzorca ataku względem zewnętrznych źródeł danych o zagrożeniach,
146) System powinien być wyposażony w funkcjonalność lub odrębne rozwiązanie pozwalające na zarządzanie ryzykiem związanym z monitorowanymi urządzeniami sieciowymi,
147) W przypadku, gdy funkcjonalność analizy ryzyka dostarczona będzie jako odrębne narzędzie, powinno być ono zintegrowane z systemem analiz i korelacji zdarzeń na poziomie danych (korzystanie z danych zgromadzonych w systemie) oraz interfejsu użytkownika (jako minimum uruchomienie mechanizmów dochodzeń z konsoli systemu analiz i korelacji zdarzeń),
148) Mechanizm zarządzania ryzykiem powinien wykorzystywać informacje zgromadzone w systemie dotyczące zdarzeń i przepływów,
149) Mechanizm powinien monitorować topologię sieciową, konfiguracje urządzeń sieciowych (w tym przełączniki, routery, firewalle, mechanizmy detekcji i zapobiegania intruzom - IPS) w celu oceny ryzyka dla konkretnego środowiska,
150) Mechanizm powinien symulować ataki sieciowe i modelować zmiany konfiguracji celem oceny ich wpływu na bezpieczeństwo,
151) Mechanizm powinien dostarczać informacji o ryzyku w formie wizualnej, powinien obrazować topologię sieciową oraz przepływy danych,
152) Mechanizm powinien zapewniać analizę podatności elementów sieci i ich konfiguracji względem możliwych ścieżek dojścia do zasobów istotnych dla organizacji oraz symulację rozprzestrzeniania się ataku,
153) Mechanizm powinien zapewnić możliwość analizy konfiguracji i polityk firewalli, w tym wykrycia ukrytych reguł i błędów oraz symulacji zmian polityk firewalla wraz z oceną ryzyka tej zmiany,
154) Wykrywanie i rejestrowanie dla celów audytowych zmian w konfiguracji urządzeń sieciowych, zawiadamianie użytkowników o działaniu niezgodnym ze zdefiniowanymi politykami (zasadami),

21. Usługa instalacji, konfiguracji i uruchomienia w/w środowiska wg. zakresu:
    a) wizja lokalna w miejscach instalacji,
    b) projekt techniczny zawierający analizę infrastruktury fizycznej i logicznej, przygotowanie kompletnej dokumentacji implementacyjnej,
    c) instalacja fizyczna sprzętu w siedzibach Zamawiającego,
    d) konfiguracja urządzeń i instalacja oprogramowania zgodnie z projektem,
    e) przygotowanie scenariuszy i przeprowadzenie testów akceptacyjnych,
    f) przygotowanie dokumentacji powykonawczej i utrzymaniowej,
22. W ramach przygotowania do obsługi dostarczanego przedmiotu zamówienia Wykonawca zapewni następujące warsztaty:
    a) przedwdrożeniowy z architektury dostarczanego systemu SIEM (1 dzień);
    b) z zarządzania i administracji systemem SIEM przeprowadzone w Autoryzowanym Ośrodku Szkoleniowym producenta (ATC) przez certyfikowaną kadrę dydaktyczną dla 6 osób (2 edycje dla 3 osób) w ukompletowaniu:
       - QRadar SIEM Foundations,
       - QRadar SIEM Administration
       - QRadar SIEM Advanced Topics
       lub równoważne w zakresie dostarczanego systemu SIEM;
    c) z zarządzania i administracji systemem SIEM dla 6 osób (2 edycje dla 3 osób) w zakresie:
       - QRadar SIEM Vulnerability Manager
       lub równoważne w zakresie dostarczanego systemu SIEM;

Załącznik nr 3 do SIWZ

spr. nr 189/Ctr/18/AK/PMP

PROJEKT UMOWY

PROGRAM MODERNIZACJI
Policii na lata 2017-2020

Egz. nr ____

U M O W A (projekt) nr .....
zawarta w Warszawie w dniu ..... 2018 r.

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..... – Zastępcę Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji

oraz przy kontrasygnacie:
1..... – Zastępcy Dyrektora Biura Finansów Komendy Głównej Policji
2.....– Naczelnika Wydziału Finansowo-Księgowego Biura Finansów Komendy Głównej Policji

a
firmą .....z siedzibą: w ....., przy ul. ....., wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla ....., ... Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS ....., NIP ....., zwaną w treści umowy **„Wykonawcą"**, reprezentowaną przez:
..... – .....
zwanych dalej łącznie **„Stronami"**.

Umowa zostaje zawarta na podstawie przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie zamówienia przetargu nieograniczonego (nr sprawy __/BŁiI/18/__) zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 z późn. zm.).

§ 1

Na potrzeby Umowy Zamawiający oraz Wykonawca ustanawiają wspólnie następujące definicje pojęć występujących w Umowie:

Skrót/pojęcie	**Definicja**
Awaria	Oznacza Awarię Krytyczną, Awarię Zwykłą.
Awaria Krytyczna	Oznacza uniemożliwienie użytkownikom lub administratorom korzystania z Systemu. Awarie krytyczne maja jedna lub więcej z poniższych cech: 1) dane przetwarzane przez System zostały uszkodzone; 2) Funkcjonalność oprogramowania nie działa; 3) System przerywa funkcjonowanie i pomimo prób nie ma możliwości jego uruchomienia,
Awaria Zwykła	Oznacza awarię nie będącą awarią krytyczną, pozwalająca na dalsze korzystanie z systemu jednakże konieczna do usunięcia.
Dane	Należy przez to rozumieć dane dotyczące abonenta, o których mowa w art. 161 ust. 2 pkt. 4–6 oraz art. 169 ust. 1 ustawy z dnia 16 lipca 2004 r. — Prawo telekomunikacyjne;

Skrót/pojęcie	Definicja
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8.15 do 16.15;
Reakcja wsparcia technicznego	Rozumiana jako przystąpienie do usunięcia awarii lub zaistniałych nieprawidłowości .
Sprzęt	Należy przez to rozumieć Przedmiot umowy określony w Załączniku nr 1 do Umowy pkt 19) i 20)

Pozostałe pojęcia użyte w Umowie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

§ 2
Przedmiot umowy

1. Przedmiotem Umowy jest **zakup: „Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management)".**
2. Szczegółowy opis przedmiotu Umowy zawiera Załączniki nr 1 do Umowy.
3. W celu uniknięcia wątpliwości Strony potwierdzają, że – z zastrzeżeniem zmian dopuszczalnych przez przepisy prawa i Umowę – przedmiot Umowy zostanie zrealizowany zgodnie z treścią Załącznika nr 1, z uwzględnieniem wszelkich zmian oraz wyjaśnień udzielonych w odpowiedzi na pytania Wykonawców, które miały miejsce w toku postępowania poprzedzającego zawarcie Umowy.
4. Specyfikacja cenowa zostaje zawarta w Załączniku nr 2 do Umowy.
5. Postanowienia Umowy obowiązują z dniem jej zawarcia.

§ 3
Organizacja Projektu

1. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Zamawiający na Kierownika Projektu wyznacza: .....
2. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Wykonawca na Kierownika Projektu wyznacza: .....
3. Kierownicy Projektu, o których mowa w ust. 1 i 2 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. Kierownicy Projektu mogą delegować swoje obowiązki na osobę trzecią. W takim przypadku muszą powiadomić Kierownika Projektu drugiej Strony z co najmniej 3-dniowym (trzy Dni Robocze) wyprzedzeniem. Zmiana taka nie wymaga aneksu do Umowy.
6. Korespondencja pomiędzy przedstawicielami Stron odbywać się będzie pisemnie oraz za pomocą: poczty elektronicznej, poczty kurierskiej lub faksów.

§ 4
Warunki płatności

1. Wartość Przedmiotu umowy, określonego w § 2, Strony ustalają na kwotę netto ..... **zł** (słownie: ..... złotych .....), co wraz z podatkiem VAT stanowi łącznie ..... **zł** brutto (słownie: ..... złotych .....).

2. 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 określonych Umową lokalizacji. Wynagrodzenie wyczerpuje wszelkie należności Wykonawcy wobec Zamawiającego związane z realizacją Umowy. Wykonawcy nie przysługuje zwrot od Zamawiającego jakichkolwiek dodatkowych kosztów, opłat i podatków poniesionych przez Wykonawcę w związku z realizacją Umowy.
3. Zamawiający opłaci należność za wykonanie Przedmiotu umowy na podstawie prawidłowo wystawionych przez Wykonawcę faktur VAT.
4. Podstawą wystawienia faktury za wykonanie Przedmiotu umowy będzie, podpisany bez zastrzeżeń przez komisję Zamawiającego i przedstawicieli Wykonawcy, protokół odbioru Przedmiotu Umowy, którego wzór stanowi Załącznik nr 5 do Umowy.
5. Wykonawca wystawi faktury VAT wskazując jako płatnika:

Komendę Główną Policji

02-624 Warszawa, ul. Puławska 148/150

NIP 521-31-72-762, REGON 012137497

6. Płatność dokonana będzie na rzecz Wykonawcy przelewem bankowym na rachunek wskazany na fakturze VAT, w ciągu 30 (trzydziestu) dni od daty dostarczenia prawidłowo wystawionej faktury VAT.
7. Za datę zapłaty przyjmuje się datę obciążenia przez bank rachunku Zamawiającego. Zamawiający upoważnia Wykonawcę do wystawienia faktury VAT bez podpisu Zamawiającego.
8. Wszelkie rozliczenia finansowe między Zamawiającym, a Wykonawcą będą prowadzone wyłącznie w złotych polskich.
9. Wykonawca przed zawarciem Umowy wniósł zabezpieczenie należytego wykonania Umowy w formie ..... w wysokości 10% wartości brutto Umowy tj. kwotę ..... (słownie złotych: .....).
10. Zabezpieczenie należytego wykonania Umowy zostanie zwrócone w następującym terminie:
    a) 70% zabezpieczenia należytego wykonania Umowy, tj. kwotę ..... zł (słownie złotych: .....) gwarantującą zgodne z Umową wykonanie Przedmiotu umowy, w terminie 30 dni od dnia wykonania Umowy i uznania przez Zamawiającego za należycie wykonaną,
    b) 30% zabezpieczenia należytego wykonania Umowy, tj. kwotę ..... (słownie złotych: .....), nie później niż 15 dni po upływie okresu rękojmi.
11. Wniesione przez Wykonawcę zabezpieczenie jest przeznaczone na pokrycie roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, w tym roszczeń z tytułu rękojmi za wady.
12. 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.
13. 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.
14. Wykonawca oświadcza, że wyraża zgodę na bezpośrednie potrącenie przez Zamawiającego z zabezpieczenia wszelkich należności powstałych w wyniku niewykonania lub nienależytego wykonania Umowy.

§ 5

Wykonanie i realizacja Umowy

1. Wykonawca zobowiązuje się do realizacji Przedmiotu Umowy w terminie do dnia ***17 grudnia 2018r.***
2. Wykonawca w terminie do 7 dni od daty zawarcia Umowy przedstawi Zamawiającemu plan wdrożenia z uwzględnieniem:
   1) przeprowadzenia warsztatów przedwdrożeniowych, trwających 1 dzień, z architektury dostarczonego systemu SIEM. Warsztaty muszą odbyć się na minimum 3 dni przed planowanym wdrożeniem;
   2) instalacji, konfiguracji uruchomienia systemu zgodnie z opisem Przedmiotu Umowy;
   3) przeprowadzenia warsztatów z zarządzania i administracji systemem SIEM zgodnie z opisem Przedmiotu Umowy;
3. Zamawiający dokona akceptacji planu wdrożenia, o którym mowa w ust. 2, w terminie do 3 dni roboczych od jego otrzymania.
4. Wszystkie czynności o których mowa w ust. 2. pkt 1), 2) oraz 3) muszą zostać zakończone w terminie wskazanym w ust. 1.
5. Wykonawca zobowiązuje się wykonać Umowę przy zachowaniu należytej staranności, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej i stosowanymi normami technicznymi.
6. Przy wykonaniu Przedmiotu umowy, Wykonawca zobowiązuje się przestrzegać odpowiedniej organizacji prac związanych z realizacją Umowy tak, aby zapewnić terminowe wykonanie Umowy oraz delegować do prac objętych Umową osoby posiadające niezbędne uprawnienia i kwalifikacje.
7. Wykonawca na potrzeby odbioru Przedmiotu umowy dostarczy warunki licencji dla Przedmiotu umowy, opisanego w Załączniku nr 1 do Umowy.
8. Wykonawca oświadcza, że:
   1) posiada wiedzę, doświadczenie, urządzenia i narzędzia informatyczne niezbędne do prawidłowego wykonania Umowy,
   2) personel Wykonawcy wykonujący prace w ramach realizacji Umowy posiada doświadczenie i kwalifikacje niezbędne do prawidłowego wykonania Umowy.
9. Wykonawca zobowiązuje się do zapewnienia we własnym zakresie i na swój koszt wszystkich ewentualnych pozwoleń, koncesji, certyfikatów bezpieczeństwa wymaganych przez obowiązujące przepisy prawa w zakresie niezbędnym do prawidłowej realizacji Umowy oraz zobowiązuje się do oznakowania dokumentacji.
10. W przypadku powierzenia wykonania Umowy podwykonawcom, Wykonawca odpowiada za czynności wykonane przez podwykonawców oraz jego personel, jak za działania i zaniechania własne.
11. Wykonawca zobowiązany jest do ścisłej współpracy z Zamawiającym i niezwłocznego informowania Zamawiającego o wszelkich okolicznościach, mogących mieć wpływ na prawidłowość i terminowość realizacji Umowy, jednak nie później niż w terminie 2 dni od dnia ich zaistnienia, na adres e-mail osoby wskazanej w § 3 ust. 1 Umowy, a także do umożliwienia Zamawiającemu bieżącej kontroli realizacji Umowy, w formach i terminach wyznaczonych przez Zamawiającego, o ile nie wpłynie to na terminowe i należyte wykonanie Umowy przez Wykonawcę.
12. Wykonawca oraz personel wykonawcy, odpowiedzialny za realizację obowiązków wynikających z Umowy, zobowiązany jest do przestrzegania wszystkich wewnętrznych regulaminów i zasad dotyczących pracy na terenie pomieszczeń wykonywania prac, o których zostanie poinformowany przez Zamawiającego przed przystąpieniem do realizacji Umowy.
13. Zamawiający zobowiązuje się udostępnić na wniosek Wykonawcy niezbędne dane i informacje warunkujące wykonanie Umowy (architektura sieci, miejsca włączenia urządzeń itp.) w możliwie najkrótszym terminie.

14. Przedmiot umowy będzie podlegać odbiorowi zgodnie z procedurą odbioru opisaną w Załączniku nr 3.
15. Wszystkie czynności związane z odbiorami muszą się zakończyć w terminie wskazanym w ust.1.
16. W ramach realizacji Przedmiotu umowy Zamawiający zastrzega sobie prawo ostatecznej akceptacji osób ze strony Wykonawcy wyznaczonych do realizacji Umowy.
17. Zamawiający będzie współpracował z Wykonawcą w celu umożliwienia Wykonawcy realizacji jego zobowiązań wynikających z postanowień Umowy, a w szczególności zapewni pomoc ze strony swojego personelu niezbędną do realizacji zobowiązań Wykonawcy.

§ 6

Wymagania dotyczące gwarancji

1. Szczegółowe warunki gwarancyjne zawiera Załącznik nr 4.
2. Bieg okresu gwarancyjnego rozpocznie się od daty podpisania bez zastrzeżeń protokołu odbioru Przedmiotu umowy, którego wzór stanowi Załącznik nr 5 do Umowy.
3. Strony ustalają okres rękojmi równy okresowi gwarancji.

§ 7

Kary umowne

1. Wykonawca odpowiada za szkodę wyrządzoną Zamawiającemu, 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. Wykonawca zobowiązuje się zapłacić Zamawiającemu następujące kary umowne:
   1) 10% wartości brutto Przedmiotu umowy z tytułu odstąpienia od Umowy w całości lub części przez Zamawiającego lub Wykonawcę z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy;
   2) 1000,00 zł brutto w przypadku przekroczenia terminu realizacji Przedmiotu umowy za każdy rozpoczęty dzień opóźnienia;
   3) 10% wartości brutto Przedmiotu umowy w przypadku udostępnienia osobom trzecim przez Wykonawcę lub osoby, którymi się posługuje przy realizacji Umowy informacji poufnych Zamawiającego, w wyniku naruszenia przez Wykonawcę zasad poufności określonych w § 8 Umowy.
   4) 1.000 zł brutto za każdą godzinę opóźnienia z tytułu przekroczenia wymaganego czasu usunięcia awarii krytycznej,
   5) 300 zł brutto z tytułu przekroczenia wymaganego czasu usuwania awarii zwykłej, za każdy rozpoczęty dzień opóźnienia.
3. Zapłata kar umownych o których mowa w ust. 2 pkt 2), 3), 4),5) nie zwalnia Wykonawcy z obowiązku wykonania Przedmiotu umowy.
4. Kary umowne podlegają łączeniu.
5. Zamawiający jest uprawniony do potrącenia 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. Prawo naliczenia kar umownych, o których mowa w ust. 2, nie ma zastosowania w przypadku gdy opóźnienie wynika wyłącznie z winy Zamawiającego.
7. 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.

8. Żadna ze Stron nie ponosi odpowiedzialności za częściowe lub całkowite niewykonanie zobowiązań wynikających z niniejszej Umowy, jeżeli to niewykonanie jest następstwem zdarzenia zewnętrznego, którego skutków Strony wcześniej nie mogły przewidzieć – w świetle obiektywnej oceny sytuacji - ani im zapobiec przy dochowaniu należytej staranności („Siła Wyższa").

9. Strona, która nie podejmie lub nie wykona swoich obowiązków zawiadomi na piśmie drugą Stronę o niewykonaniu lub zawieszeniu wykonywania swoich obowiązków z powodu Siły Wyższej.

10. Za Siłę Wyższą nie uznaje się niedotrzymania zobowiązań przez kontrahenta – dostawcę Wykonawcy.

11. Powiadomienie, o którym mowa w ust. 9 zostanie dokonane przez Strony nie później niż w terminie 4 (czterech) dni od wystąpienia zdarzenia zewnętrznego.

12. W przypadku działania Siły Wyższej, ustalony w niniejszej Umowie czas przeznaczony na wykonanie Przedmiotu Umowy zostanie przedłużony o czas działania Siły Wyższej lub jej skutków.

13. Jeżeli okres ten będzie przekraczał 2 (dwa) miesiące, Strony w odrębnym trybie podejmą decyzję w sprawie sposobu wykonania niniejszej Umowy.

§8

Poufność

1. Wykonawca i Zamawiający zobowiązują się do zachowania w poufności informacji otrzymanych od drugiej Strony i z zastrzeżeniem wyjątków określonych w Umowie lub obowiązujących przepisach prawa, nie udostępniania tych informacji osobom trzecim bez zgody danej Strony.

2. Wykonawca zobowiązuje się dotrzymać tajemnicy i poufności informacji uzyskanych w trakcie wykonania tej Umowy oraz nie ujawniać ich komukolwiek poza uprawnionymi pracownikami Wykonawcy i tylko w celu prawidłowego wykonania tej Umowy.

3. Za informacje poufne nie będą uważane informacje, które druga ze Stron już posiada, które są publicznie znane, które zostały przez drugą Stronę niezależnie wypracowane lub które uzyskała ona zgodnie z prawem i bez klauzuli zachowania tajemnicy handlowej od osób trzecich, jak też informacje, których ujawnienie wymagane jest przez bezwzględnie obowiązujące przepisy prawa oraz informacje ujawnione za uprzednią pisemną zgodą Strony.

4. Z zastrzeżeniem innych postanowień Umowy, informacje poufne uzyskane przez Strony w związku z wykonywaniem Umowy nie mogą być ujawniane bez pisemnej zgody drugiej Strony.

5. Z zastrzeżeniem innych postanowień Umowy oraz sytuacji, gdy jest to potrzebne do zawarcia lub wykonania Umowy, zobowiązanie do zachowania poufności obejmuje:

   1) zakaz kopiowania i powielania informacji poufnych otrzymanych od drugiej Strony jakąkolwiek techniką;

   2) zakaz informowania w sposób pośredni ani bezpośredni jakichkolwiek osób nieupoważnionych o fakcie posiadania informacji poufnych otrzymanych od drugiej Strony i ich treści;

   3) zakaz przekazywania i udostępniania informacji poufnych otrzymanych od drugiej Strony w sposób pośredni lub bezpośredni osobom nieupoważnionym;

   4) zapewnienie pełnego bezpieczeństwa posiadanych informacji i danych poufnych otrzymanych od drugiej Strony przed dostępem osób trzecich, zwłaszcza poprzez odpowiednie ich przechowywanie zabezpieczające przed zapoznaniem się z ich treścią, skopiowaniem lub zabraniem przez osoby nieupoważnione.

6. Każda ze Stron może na żądanie właściwego sądu, organu administracyjnego lub innych upoważnionych organów udostępnić im informacje dotyczące drugiej Strony w zakresie wskazanym w takim żądaniu.

7. Z zastrzeżeniem postanowienia poniżej, w przypadku rozwiązania lub wygaśnięcia Umowy oraz w przypadku odstąpienia od Umowy Strony są zobowiązane do zwrotu lub do zniszczenia wszelkich materiałów, jakie otrzymały w związku z wykonywaniem Umowy.
8. Postanowienia niniejszego paragrafu dotyczą również osób fizycznych.
9. Określone w niniejszym paragrafie zobowiązanie do zachowania w poufności informacji poufnych obowiązywać będzie w czasie trwania Umowy oraz w terminie 3 lat od daty zakończenia Umowy, o ile przepisy powszechnie obowiązujące nie przewidują dłuższych okresów ich ochrony.
10. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób z jego strony, uprawnionych do realizacji Przedmiotu umowy określonego w § 2 ust. 1.
11. W celu zapewnienia kontroli osób uzyskujących dostęp do policyjnych zasobów, w tym Aktywów Teleinformatycznych, Wykonawca wraz z listą osób dostarczy:
    1) dla każdej osoby zgłoszonej do realizacji Umowy kserokopię aktualnego zaświadczenia o niekaralności potwierdzonego za zgodność z oryginałem wystawionego nie wcześniej niż 3 miesiące przed dniem zawarcia Umowy lub alternatywnie dokument elektronicznie wygenerowany przez system e-Platforma Ministerstwa Sprawiedliwości. Kierowane do Krajowego Rejestru Karnego zapytanie o udzielenie informacji o osobie, powinno dotyczyć kartoteki karnej. Ponadto w ww. formularzu nie należy wypełniać pkt 11 pn. *Wskazanie postępowania, w związku z którym zachodzi potrzeba uzyskania informacji o osobie*;
    2) oświadczenie o zachowaniu poufności dla każdej osoby realizującej Umowę, którego wzór określa Załącznik nr 9 do Umowy.
    3) oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO , który wzór określa załącznik nr 10 Umowy.
12. Zamawiający dopuści do realizacji Przedmiotu Umowy jedynie osoby spełniające warunki określone w ust. 11.
13. Podczas wykonywania Umowy Wykonawca nie będzie miał dostępu do informacji niejawnych w rozumieniu przepisów Ustawy z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r. poz. 412).

§ 9

Odstąpienie od Umowy

1. Zamawiający zastrzega sobie prawo do odstąpienia od Umowy w szczególności w przypadku:
    1) wystąpienia istotnej zmiany okoliczności powodującej, 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;
    2) opóźnienia w wykonaniu Przedmiotu umowy trwającego dłużej niż 5 dni roboczych, bez wyznaczania stronie dodatkowego terminu na wykonanie. Oświadczenie o odstąpieniu, o którym mowa w zdaniu poprzednim, winno być złożone przez Zamawiającego w terminie do 14 dni roboczych od dnia w którym upłynął 5 dniowy termin opóźnienia w stosunku do terminu wskazanego w § 5 ust. 1;
    3) dostarczenia Przedmiotu umowy niespełniającego wymogów określonych w Załączniku nr 1 do Umowy. Oświadczenie o odstąpieniu, o którym mowa poprzednim punkcie, winno być złożone przez Zamawiającego w terminie 14 Dni Roboczych od dnia dostarczenia przez Wykonawcę;
    4) jeżeli suma kar umownych naliczonych na podstawie Umowy przekroczy wartość wynagrodzenia brutto określonego w § 4 ust. 1 Umowy;
2. Odstąpienie 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. 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).

§10

Zmiany Umowy

1. Strony są uprawnione do wprowadzenia do Umowy zmian nieistotnych, to jest innych, niż zmiany zdefiniowane w art. 144 ust. 1e Ustawy Pzp.

2. Stosownie do art. 144 ust. 1 pkt 1 Ustawy Pzp, Zamawiający przewiduje możliwość wprowadzenia do Umowy zmian opisanych w ustępach poniżej:

   1) w przypadku wprowadzenia przez producenta nowej wersji oprogramowania/sprzętu lub innych produktów, Zamawiający dopuszcza zmianę wersji oprogramowania/sprzętu lub Produktu pod warunkiem, że nowa wersja spełnia wymagania określone w SIWZ i nie powodują zmiany ceny;

   2) w przypadku zakończenia wytwarzania oprogramowania/sprzętu lub innego produktu objętego Umową lub wycofania ich z produkcji lub z obrotu na terytorium Rzeczypospolitej Polskiej, Zamawiający dopuszcza zmianę polegającą na dostarczeniu produktu zastępczego o parametrach spełniających wymagania określone w SIWZ i nie powodują zmiany ceny;

   3) w przypadku zmiany przepisów prawa, opublikowanej w Dzienniku Urzędowym Unii Europejskiej, Dzienniku Ustaw, Monitorze Polskim lub Dzienniku Urzędowym odpowiedniego ministra, Zamawiający dopuszcza zmiany sposobu realizacji Umowy lub zmiany zakresu świadczeń Wykonawcy wymuszone takimi zmianami prawa;

   4) w przypadku ujawnienia się powszechnie występujących wad oferowanego oprogramowania/sprzętu lub urządzenia Zamawiający dopuszcza zmianę w zakresie Przedmiotu umowy polegającą na zastąpieniu danego produktu produktem zastępczym, spełniającym wszelkie wymagania przewidziane w SIWZ dla produktu zastępowanego, rekomendowanym przez producenta lub wykonawcę w związku z ujawnieniem wad;

   5) w przypadku wystąpienia zależności realizacji Przedmiotu umowy od wyników innych projektów teleinformatycznych, w takim przypadku Zamawiający zastrzega sobie możliwość wydłużenia terminu realizacji Umowy;

   6) w przypadku przedłużającej się procedury udzielenia zamówienia publicznego na skutek korzystania przez Wykonawców ze środków ochrony prawnej, Zamawiający dopuszcza zmiany terminu wykonania Przedmiotu umowy. W takim przypadku Zamawiający zastrzega sobie możliwość wydłużenia terminu realizacji Umowy o czas trwania procedury odwoławczej.

3. Strony postanawiają, że w przypadku zmiany stawki podatku od towarów i usług – Wynagrodzenie przewidziane niniejszą Umową ulegnie zmianie odpowiedniej do zmiany wysokości podatku od towarów i usług (ulegnie korekcie o wysokość zmiany podatku VAT), przy czym powyższa zmiana będzie miała zastosowanie wyłącznie w odniesieniu do części Wynagrodzenia objętego fakturami wystawionymi po dacie wejścia w życie zmiany przepisów prawa wprowadzających nowe stawki podatku od towarów i usług.

4. Zmiany, o których mowa powyżej wymagają zgody obu Stron i muszą być dokonywane w formie pisemnej pod rygorem nieważności w postaci aneksu.

§ 11

Licencje

1. Z chwilą podpisania protokołu odbioru Przedmiotu umowy, w ramach wynagrodzenia wskazanego w § 4 ust. 1 Umowy Wykonawca zapewnia Zamawiającemu nieograniczone terytorialnie i czasowo licencje udzielone przez producenta tego oprogramowania, których warunki tenże producent dołączył do oprogramowania, bezterminowe, niewyłączne prawo do korzystania z Licencji do Oprogramowania jest na następujących polach eksploatacji:
   a) prawo do korzystania z wszystkich funkcjonalności Oprogramowania, do którego zostały dostarczone w ramach Umowy Licencje, w dowolny sposób w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej dla dostarczonych Licencji do Oprogramowania;
   b) prawo do instalowania Oprogramowania, do którego zostały dostarczone w ramach Umowy Licencje, w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej dla dostarczonych Licencji do Oprogramowania;
   c) prawo do instalowania wszelkich poprawek i uaktualnień opublikowanych na stronach producenta Oprogramowania oraz polach eksploatacji określonych w opublikowanych przez producenta warunkach licencyjnych;
   d) instalowanie i deinstalowanie Oprogramowania pod warunkiem zachowania liczby udzielonych Licencji;
   e) prawo do utrwalania przez Zamawiającego Oprogramowania, do którego zostały dostarczone w ramach Umowy Licencje, na nośnikach.
2. Wykonawca oświadcza, że uzyskał zgodę producenta na korzystanie z Oprogramowania określonego w Załączniku nr 1 do Umowy, w tym na przekazywanie dokumentów zawierających warunki licencji.
3. W okresie od dnia dostarczenia do Zamawiającego Oprogramowania, o którym mowa w Załączniku nr 1 do Umowy, w sposób określony w Umowie, do dnia podpisania protokołu odbioru Przedmiotu umowy, Wykonawca zapewni Zamawiającemu korzystanie z tego Oprogramowania na warunkach licencji, bez pobierania z tego tytułu dodatkowego wynagrodzenia.
4. Udzielenie Zamawiającemu Licencji do Oprogramowania następuje z chwilą podpisania przez Strony protokołu Przedmiotu umowy.
5. 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.
6. 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, ani praw do baz danych.
7. 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.
8. 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.

9. 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 Umowy.

§ 12
Własność

1. Wszelkie dokumenty i materiały będące własnością Zamawiającego, a przekazane Wykonawcy w celu umożliwienia mu prawidłowej realizacji Umowy, pozostają wyłączną własnością Zamawiającego.
2. Wykonawca nie może udostępniać materiałów, dokumentów, o których mowa w ust. 1 powyżej, osobom trzecim, nie może także ich powielać w całości ani w części bez uzyskania wcześniejszej pisemnej zgody Zamawiającego.
3. Wykonawca zobowiązuje się zwrócić Zamawiającemu wszelkie dokumenty i materiały będące własnością Zamawiającego, o których mowa w ust. 1 powyżej wraz ze wszystkimi kopiami oraz nośnikami, na których dokumenty zostały zapisane w wersji elektronicznej, niezwłocznie po wykonaniu Umowy.

§ 13
Postanowienia końcowe

1. Wykonawca ma prawo powierzać wykonanie świadczeń objętych Przedmiotem Umowy osobom fizycznym współpracującym z Wykonawcą. Wykonawca może skorzystać z podwykonawcy wyłącznie w zakresie, który wskazał w swojej ofercie. Wykonawca może dokonać zamiany podwykonawcy po pisemnym poinformowaniu o tym Zamawiającego (z podaniem przyczyn zamiany) i uzyskaniu jego zgody na zamianę podwykonawcy. W przypadku, gdy Wykonawca będzie korzystał z podwykonawcy, zobowiązany jest do niezwłocznego pisemnego powiadomienia Zamawiającego, poprzez wskazanie nazwy tego podwykonawcy. Wykonawca powierzając podwykonawcy lub osobom fizycznym współpracującym z Wykonawcą do wykonania Przedmiot Umowy odpowiada za jego działania, jak za działania własne.
2. Wszelkie zmiany i uzupełnienia w niniejszej Umowie mogą być dokonywane za zgodą obu Stronna piśmie pod rygorem nieważności w postaci aneksu.
3. Wykonawca nie może bez pisemnej – pod rygorem nieważności – i uprzedniej zgody Zamawiającego przenieść na osobę trzecią żadnej wierzytelności wynikającej z Umowy.
4. W sprawach nieuregulowanych w Umowie zastosowanie mieć będą przepisy ustawy Kodeks Cywilny, ustawy o prawie autorskim i prawach pokrewnych, ustawy prawo zamówień publicznych i ustawy o ochronie informacji niejawnych.
5. Spory związane z Umową będą rozstrzygane przez Strony w trybie porozumienia Stron w terminie 14 (czternastu) dni, licząc od otrzymania pisemnego wystąpienia jednej ze Stron.
6. Strony dołożą starań w celu rozstrzygnięcia sporów za porozumieniem Stron w najkrótszym terminie i w sposób rzetelny.
7. W przypadku nieosiągnięcia porozumienia w terminie, o którym mowa w ust. 5, Strony bezzwłocznie ustalą na piśmie dalszy tryb postępowania w celu ugodowego rozstrzygnięcia sporu.
8. W przypadku nieosiągnięcia porozumienia, co do trybu, o którym mowa w ust 7 sprawy rozstrzygać będzie Sąd powszechny, miejscowo właściwy dla Zamawiającego.
9. Wykaz Załączników stanowiących integralną część Umowy:

Załącznik nr 1 – Opis Przedmiotu umowy;

Załącznik nr 2 – Specyfikacja ilościowo-cenowa;

Załącznik nr 3 – Zasady odbioru Przedmiotu umowy;

Załącznik nr 4 – Wymagania gwarancyjne;

Załącznik nr 5 – Wzór Protokołu odbioru Przedmiotu Umowy;

Załącznik nr 6 – Wzór protokołu odbioru Dokumentu;

Załącznik nr 7 – Wzór Protokołu odbioru ilościowego;

Załącznik nr 8 – Wzór protokołu odbioru jakościowego;

Załącznik nr 9 – Oświadczenie o zachowaniu poufności

Załącznik nr 10 – Oświadczenie o wypełnieniu obowiązku informacyjnego RODO

Załącznik nr 11 – Wzór protokołu odbioru warsztatów szkoleniowych

10. Umowę sporządzono w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający a 1 (jeden) egzemplarz Wykonawca.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1 do Umowy

Szczegółowy Opis Przedmiotu umowy
(zostanie sporządzony na podstawie OPZ oraz formularza ofertowego wykonawcy)

Załącznik nr 2 do Umowy

SPECYFIKACJA ILOŚCIOWO-CENOWA

Lp.	*Opis*	*Ilość*	*Wartość netto*	*VAT*	*Wartość brutto*
1.					

Załącznik nr 3 do Umowy

SZCZEGÓŁOWE ZASADY ODBIORU PRZEDMIOTU UMOWY

I. Zasady ogólne

1. O przygotowaniu do odbioru Przedmiotu Umowy, Wykonawca powiadomi Wydział Zarządzania Projektami BŁiI KGP faksem na numer 22 60 158-73, podając:
   - numer Umowy,
   - planowaną datę przystąpienia do odbioru,
2. Zamawiający przystąpi do odbioru Przedmiotu umowy w ciągu 5 (pięciu) Dni Roboczych od otrzymania od Wykonawcy zgłoszenia gotowości do odbioru.
3. Odbiór zostanie przeprowadzony przez Komisję do odbioru Przedmiotu umowy Zamawiającego w obecności przedstawicieli Wykonawcy w Warszawie, w obiekcie wskazanym przez Zamawiającego.
4. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy Protokołu odbioru Przedmiotu Umowy, którego wzór stanowi Załącznik nr 5 do Umowy.
5. Odbiór Przedmiotu Umowy będzie poprzedzony odbiorami: dokumentu, jakościowym ilościowym oraz warsztatów szkoleniowych.
6. Wykonawca przed przystąpieniem do odbioru zobowiązany jest do wypełnienia i dostarczenia Zamawiającemu protokołów, o których mowa w Załącznikach nr 6, nr 7, nr 8 oraz nr 11 do Umowy.
7. Wszystkie protokoły, sporządzone zostaną w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający a 1 (jeden) egzemplarz otrzymuje Wykonawca.

II. Odbiór dokumentu.

1. Celem czynności kontrolnych prowadzonych w ramach odbioru dokumentu jest sprawdzenie całości dostarczonej dokumentacji pod względem wymagań oraz zgodności z Umową jak również opisem przedmiotu Umowy, wyszczególnionym w Załączniku nr 1 do Umowy.
2. Pozytywny wynik odbioru dokumentu zostanie potwierdzony podpisaniem protokołu odbioru dokumentu, który stanowi Załącznik nr 6 do Umowy.

III. Odbiór jakościowy.

2. Odbiór jakościowy będzie przeprowadzony w Komendzie Głównej Policji w Warszawie.
3. Celem czynności kontrolnych prowadzonych w ramach odbioru jakościowego jest sprawdzenie wszystkich wymagań funkcjonalnych dostarczonego Przedmiotu Umowy i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
4. Podstawą dokonania odbioru jakościowego w KGP jest przeprowadzenie, z pozytywnym skutkiem, Testów Akceptacyjnych według Planu Testów Akceptacyjnych oraz Scenariuszy Testów Akceptacyjnych.

5. Plan Testów Akceptacyjnych i Scenariusze Testów Akceptacyjnych Wykonawca przekazuje Kierownikowi Projektu Zamawiającego nie później niż 5 (pięć) dni kalendarzowych przed zgłoszeniem gotowości Wykonawcy do odbiorów jakościowych.
6. Plan Testów Akceptacyjnych i Scenariusze Testów Akceptacyjnych zostaną poddane weryfikacji przez Zamawiającego w ciągu 3 (trzech) Dni Roboczych od daty ich przekazania przez Wykonawcę do Zamawiającego. Zamawiający zgłasza do Wykonawcy swoje uwagi w formie elektronicznej , które zostaną przekazane przez Kierownika Projektu Zamawiającego jednorazowo. Jeżeli Zamawiający zgłosi uwagi do planu testów w okresie zdefiniowanym powyżej, Kierownik Projektu Wykonawcy określa czas ustosunkowania się Wykonawcy do uwag. Następnie Kierownicy Projektu ustalają datę dostarczenia zmodyfikowanych wersji planu testów.
7. Dla zmodyfikowanej wersji Planu Testów Akceptacyjnych oraz Scenariuszy Testów Akceptacyjnych kroki niniejszej procedury zostają powtórzone, przy czym okres weryfikacji wynosi 2 (dwa) Dni Robocze. Weryfikacji przez Zamawiającego poddawane są tylko te elementy planu testów oraz scenariuszy, które wynikają z uwag zgłoszonych przez Zamawiającego w okresie weryfikacji.
8. Pozytywny wynik odbioru jakościowego zostanie potwierdzony podpisaniem przez komisję powołaną do odbioru przedmiotu Umowy i Wykonawcę protokołu odbioru jakościowego, który stanowi Załącznik nr 8 do Umowy.

IV. Odbiór ilościowy

1. Pozytywny wynik odbioru jakościowego warunkuje przystąpienie Stron do odbioru ilościowego Przedmiotu umowy.
2. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowego jest sprawdzenie kompletności dostarczonego przedmiotu umowy i potwierdzenie zgodności z ilością określoną w umowie.
3. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego Przedmiotu Umowy.
4. Pozytywny wynik odbioru ilościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowego, którego wzór określa Załącznik nr 7 do umowy.

V. Odbiór warsztatów szkoleniowych

1. Odbiór warsztatów szkoleniowych zostanie dokonany przez komisję Zamawiającego, powołaną Decyzją Komendanta Głównego Policji, na podstawie imiennych certyfikatów/ zaświadczeń dla uczestników warsztatów szkoleniowych, wystawionych przez ośrodek szkoleniowy oraz list obecności uczestników za każdy dzień warsztatów szkoleniowych.
2. Odbiór warsztatów szkoleniowych zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego oraz Wykonawcy protokołu odbioru warsztatów szkoleniowych, którego wzór określa Załącznik nr 11 Do Umowy.

Załącznik nr 4 do Umowy

WYMAGANIA DOTYCZĄCE GWARANCJI

1. Okres gwarancji dla Sprzętu wynosi ..... (zgodnie z ofertą Wykonawcy nie mniej niż 36 miesięcy), przy czym bieg okresu gwarancji rozpocznie się z chwilą podpisania bez zastrzeżeń protokołu odbioru Przedmiotu umowy.
2. Do dostarczonego Sprzętu będą dołączone karty gwarancyjne, podlegające akceptacji Zamawiającego, zawierające numer seryjny sprzętu, termin i warunki ważności gwarancji (zgodnie z Umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
3. Całość prac związanych z fizycznym dostępem do urządzeń objętych gwarancja, będzie przeprowadzana przez zespół wykonawcy w siedzibie zamawiającego.
4. Wykonawca będzie świadczył gwarancję przez okres określony w Umowie, a w jej ramach będzie odpowiedzialny za:
   1) diagnozowanie awarii serwerów,
   2) diagnozowanie awarii macierzy,
   3) usuwanie wad ukrytych,
   4) wymianę uszkodzonych podzespołów, przy czym poniesie wszystkie związane z tym koszty a uszkodzone dyski zostają u Zamawiającego,
   5) prawidłową konfigurację sprzętu i oprogramowania systemowego.
5. Zamawiający będzie klasyfikował awarie na:
   1) Awaria krytyczna – obejmuje awarię sprzętu wyszczególnionego w specyfikacji serwerów i macierzy, czyli każdego sprzętu jako całości (każdego serwera, macierzy, itd.)
   2) Awaria Zwykła – każda awaria, która nie spełnia definicji Awarii Krytycznej obejmująca awarię sprzętu jego komponentów wyszczególnionych w specyfikacji serwerów i macierzy których użytkownik nie może obejść korzystając z innych funkcjonalności sprzętu lub zainstalowanego na nim systemu.
6. W ramach gwarancji:
   1) Zgłoszenia awarii będą przyjmowane 7 dni w tygodniu, 24 godziny na dobę,
   2) Wykonawca zapewni obsługę zgłoszeń w języku polskim,
   3) Wykonawca zapewni możliwość przyjmowania zgłoszeń od administratorów Zamawiającego pod ustalonym numerem telefonu i adresem e-mail.
      a) Zgłoszenia przez e-mail: .....
      b) Zgłoszenia telefoniczne /faksowe: .....
7. Maksymalny czas naprawy awarii od momentu zgłoszenia:
   1) o statusie krytyczna – 8 godzin, przy czym możliwe jest zastosowanie obejścia i sprowadzenie awarii krytycznej do awarii niekrytycznej,
   2) o statusie niekrytyczna – następny dzień roboczy, przy czym za dni robocze Zamawiający uważa dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy w Rzeczypospolitej Polskiej. Zgłoszenia po godzinie 17:00 będą traktowane jak zgłoszenia wykonane następnego dnia roboczego o godzinie 7:00.
8. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dla dostarczonego sprzętu.
9. W przypadku konieczności wymiany dysku twardego w okresie udzielonej gwarancji, będzie on wymieniony przez Wykonawcę na nowy lub sprawny, o nie gorszych parametrach technicznych, bez konieczności zwrotu uszkodzonego i dokonywania ekspertyzy poza siedzibą użytkownika. Zamawiający z tego tytułu nie będzie ponosił dodatkowych kosztów.

Załącznik nr 5 do Umowy

Egz. nr ___

PROTOKÓŁ ODBIORU PRZEDMIOTU UMOWY - wzór
do umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:

.....
Data dokonania odbioru:

.....
Ze strony Wykonawcy:

.....
(nazwa i adres)

.....
(osoba upoważniona do udziału w odbiorze)

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

Komisja do obioru przedmiotu zamówienia w składzie:
1.....

2. .....

3. .....

na podstawie przeprowadzonych czynności kontrolnych oraz Protokołów odbioru jakościowego / odbioru ilościowego / odbioru warsztatów szkoleniowych/ odbioru dokumentacji *, dostarczonych przez jednostki terenowe Policji* potwierdza:
1. kompletność dostarczonego przedmiotu umowy;*
2. zgodność jakości dostarczonego przedmiotu umowy;* z parametrami/funkcjonalnością z opisem przedmiotu umowy;*
3. wykonanie zamówienia zgodne z warunkami zawartymi w umowie.

Uwagi.....
.....
Podpisy Komisji do odbioru przedmiotu zamówienia:
Przewodniczący:

.....

Członkowie:

1. .....
2. .....
3.....
(ze strony Zamawiającego)

1.....
2.....
3.....
(ze strony Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 6 do Umowy

Egz. nr ___

PROTOKÓŁ ODBIORU DOKUMENTU - *wzór*
do umowy nr ..... z dnia.....r.

Miejsce dokonania odbioru:
.....
Data dokonania odbioru:
.....
Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(przedstawiciel wykonawcy)

Ze strony Zamawiającego:
Biuro Łączności i Informatyki
Komendy Głównej Policji
02-520 Warszawa, ul. Wiśniowa 58

Komisja do obioru Przedmiotu umowy w składzie:
.....
.....
.....

powołana na mocy Decyzji nr ..... z dnia ..... r. potwierdza dostarczenie dokumentu zgodnego/niezgodnego* z warunkami zawartymi w Umowie.

Lp.	Nazwa Dokumentu	Ilość	Uwagi

Uwagi**:.....

Zamawiający

Wykonawca

Podpisy Komisji do odbioru przedmiotu umowy:

Przewodniczący:

.....
Członkowie:
1. .....
2. .....
3.....
(Członkowie komisji Zamawiającego)

1.....
2.....
3.....
(upoważniony Przedstawiciel Wykonawcy)

*niewłaściwe skreślić
**wypełnić w przypadku negatywnego odbioru, podając jego szczegółowe przyczyny

Załącznik nr 7 do Umowy

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 przedmiotowej umowy jest:

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

Komisja do odbioru przedmiotu zamówienia, powołana na mocy ..... z dnia ..... przeprowadziła czynności kontrolne i potwierdza/nie potwierdza kompletność dostarczonego produktu. *

Uwagi:.....

.....

.....

Podpisy:

1. .....
2. .....
3. .....

(w imieniu Zamawiającego)

1.....
2.....
3.....

(Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 8
do projektu umowy

PROTOKÓŁ ODBIORU JAKOŚCIOWEGO - 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)

W ramach odbioru jakościowego, przeprowadzonego w ramach umowy nr ..... z dnia..... .....r. na _____, Komisja powołana na mocy Decyzji _____z dnia _____r. przeprowadziła czynności kontrolne na podstawie zatwierdzonej przez Strony umowy procedury i potwierdza zgodność jakości dostarczonego produktu z parametrami/funkcjonalnością zawartymi w opisie przedmiotu umowy.

Wynik odbioru jakościowego:
- Pozytywny*
- Negatywny*

Uwagi:.....
.....

Podpisy Komisji do odbioru przedmiotu zamówienia:

Przewodniczący:
.....

Członkowie:

1. .....
2. .....
3.....
(członkowie Komisji Przetargowej,

1.....
2.....
3.....
(Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 9 do Umowy

.....
(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 wiadomości udostępnionych przez pracowników i funkcjonariuszy BŁiI KGP oraz uzyskanych w związku z wykonywaniem Umowy nr ..... z dnia ..... zawartej pomiędzy Komendantem Głównym Policji a firmą ....., a nie podlegających wykluczeniom 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.

.....

Załącznik nr 10
do Umowy nr ...../..../BŁiI/18/...

.....
(miejscowość, data)

.....
(imię i nazwisko)

.....
(miejsce zatrudnienia)

OŚWIADCZENIE WYKONAWCY

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w związku z wykonywaniem umowy nr .....z dnia....., zawartej pomiędzy Komendą Główną Policji a firmą .....[2]

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

[2] W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa

Załącznik nr 11
do umowy nr

PROTOKÓŁ ODBIORU WARSZTATÓW SZKOLENIOWYCH (wzór)

do umowy nr ..... z dnia.....r.
na...../nazwa projektu/.....

Miejsce dokonania odbioru:.....

Data dokonania odbioru:.....

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

Termin warsztatów szkoleniowych ....
Ilość godzin warsztatów szkoleniowych: .....
Liczba uczestników warsztatów szkoleniowych:.....
Przedmiot i zakres warsztatów szkoleniowych:

_____/tytuł warsztatów szkoleniowych/_____

Na podstawie czynności odbiorczych, przeprowadzonych w ramach umowy Komisja do odbioru przedmiotu zamówienia, powołana na mocy.....z dnia ..... r. potwierdza zgodność przeprowadzonego warsztatów szkoleniowych z warunkami umowy.

Załączniki:
1. Harmonogram warsztatów szkoleniowych
2. Lista osób uczestniczących w warsztatach szkoleniowych wraz z podpisami uczestników i kopiami uzyskanych zaświadczeń potwierdzających udział w warsztatach szkoleniowych.

Uwagi:
.....
.....

Podpisy Komisji do odbioru przedmiotu zamówienia:

Przewodniczący:
.....

Członkowie:

1. ..... 1.....
2. ..... 2.....
3..... 3.....
(Członkowie komisji Zamawiającego) (upoważniony Przedstawiciel Wykonawcy)

Załącznik nr 4 do SIWZ

spr. nr 189/BŁiI18/AK/PMP

.....

pieczęć Wykonawcy

OŚWIADCZENIE O PRZYNALEŻNOŚCI LUB BRAKU PRZYNALEŻNOŚCI DO TEJ SAMEJ GRUPY KAPITAŁOWEJ

Przystępując do udziału w postępowaniu o udzielenie zamówienia pn. ***Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management)***, numer postępowania **189/BŁiI/18/AK/PMP**, prowadzonym w trybie przetargu nieograniczonego, stosownie do art. 24 ust. 1 pkt 23 ustawy Prawo zamówień publicznych (Dz. U. z 2017 r. poz.1579) oświadczam, że

1) nie należę do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r., poz.184, 1618, 1634) *

2) należę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2015 r. poz. 184, 1618 i 1634) z następującymi Wykonawcami, którzy złożyli oferty w niniejszym postępowaniu o udzielenia zamówienia*:

   1) .....
   2) .....

   oraz przedstawiam wraz z niniejszym oświadczeniem dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielnie zamówienia:
   .....
   .....,

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

.....

(podpis osoby/osób upoważnionej)

* niepotrzebne skreślić

UWAGA: Powyższe oświadczenie Wykonawca przekazuje Zamawiającemu w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy – Prawo zamówień publicznych. W przypadku przynależności do tej samej grupy kapitałowej Wykonawca wraz ze złożonym oświadczeniem może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia

Załącznik nr 5 do SIWZ
spr. nr 189/BŁiI18/AK/PMP

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest *Komendant Główny Policji ;*
- Nadzór nad prawidłowym przetwarzaniem danych osobowych w Komendzie Głównej Policji sprawuje inspektor ochrony danych osobowych KGP:
  Adres: ul. Puławska 148/150. 02-624 Warszawa
  e-mail: iod.kgp@policja.gov.pl.

Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego *Rozbudowa posiadanego przez Zamawiającego systemu do zarządzania informacją i zdarzeniami bezpieczeństwa teleinformatycznego typu SIEM (Security Information and Event Management)*, numer postępowania 189/BŁiI/18/AK/PMP prowadzonym w trybie przetargu nieograniczonego;

- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp";
- Okres przechowywania danych osobowych wynika bezpośrednio z przepisów prawa. Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, okres 4 lat może być wydłużony do zakończenia czasu trwania umowy lub w przypadku, gdy dane będą przetwarzane do celów archiwalnych w interesie publicznym.
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych [i];

- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO[ii];
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

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

---

[i] ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

[ii] ***Wyjaśnienie:*** *prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*