SPECYFIKACJA
ISTOTNYCH WARUNKÓW ZAMÓWIENIA

ZAMAWIAJĄCY:

Wojskowy Instytut Łączności

ul. Warszawska 22A, 05-130 Zegrze Południowe

Tel. 261 885 555, fax. 261 885 589

Strona internetowa www.wil.waw.pl

NIP: 524 030 70 48

PRZEDMIOT ZAMÓWIENIA:

Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych

W POSTĘPOWANIU PROWADZONYM
W TRYBIE PRZETARGU NIEOGRANICZONEGO

NR SPRAWY ZP-13-15-CYBERSECLAB

ZATWIERDZAM

.....
DYREKTOR
DR INŻ. MAREK RÓŻYCKI

PROJEKT WSPÓŁFINANSOWANY ZE ŚRODKÓW EUROPEJSKIEGO FUNDUSZU ROZWOJU REGIONALNEGO
W RAMACH PROGRAMU OPERACYJNEGO INNOWACYJNA GOSPODARKA
PROJEKT NR POIG 02.03.00-14-106/13
„Laboratorium Analiz Ataków Cybernetycznych".

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Zamawiającym jest:
Wojskowy Instytut Łączności
ul. Warszawska 22A, 05-130 Zegrze Południowe
tel. 261 885 555, fax. 261 885 589
Strona internetowa www.wil.waw.pl
NIP: 524 030 70 48

II. TRYB UDZIELANIA ZAMÓWIENIA

1. Postępowanie prowadzone jest zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r., Prawo zamówień publicznych (t. j. Dz. U. z 2013 r. poz. 907 z późn. zm.), a także wydanymi na podstawie niniejszej ustawy rozporządzeniami wykonawczymi.
2. Postępowanie prowadzone jest w trybie przetargu nieograniczonego o wartości szacunkowej poniżej progów określonych w przepisach wydanych na podstawie art. 11 ust. 8 Pzp.
3. Podstawa prawna wyboru trybu udzielania zamówienia publicznego – art. 10 ust. 1 oraz art. 39-46 Pzp.
4. **Zamówienie jest współfinansowane ze środków Unii Europejskiej w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet 2. Infrastruktura sfery B+R, Działanie 2.3: Inwestycje związane z rozwojem infrastruktury informatycznej nauki, Poddziałanie 2.3.1 Projekty w zakresie rozwoju infrastruktury informatycznej nauki, Poddziałanie 2.3.2 Projekty w zakresie rozwoju zasobów informacyjnych nauki w postaci cyfrowej, Poddziałanie 2.3.3 Projekty w zakresie rozwoju zaawansowanych aplikacji i usług teleinformatycznych, Projekt Nr POIG 02.03.00-14-106/13.**
5. Akty prawne mające istotne znaczenie przy opracowaniu niniejszej SIWZ:
   a) Ustawa z dnia 29 stycznia 2004 r., Prawo zamówień publicznych (t. j. Dz. U. z 2013 r. poz. 907 z późn. zm.).
   b) Ustawa z dnia 23 kwietnia 1964 r., Kodeks cywilny (t. j. Dz. U. z 2014 r. poz. 121).
   c) Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t. j. Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.).

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Kody klasyfikacji Wspólnego Słownika Zamówień (CPV): **80510000-2**
2. Przedmiot zamówienia:
   a) Przedmiotem zamówienia jest usługa szkolenia specjalistycznego w formie voucherów uprawniających do udziału w szkoleniach w zakresie systemów i oprogramowania specjalistycznego. Wykonawca zobowiązany jest do dostawy **voucher'ów na korzystanie z usług szkoleniowych w ww. zakresie z podziałem na zadania 1-24 wg specyfikacji w załączniku 11.**
   Przy opisie zawartości szkoleń wykorzystano źródła stron internetowych firm szkoleniowych. Zamawiający nie preferuje żadnych z tych firm.
   Zgodnie z art. 11 pkt 1, 3–7 ustawy z dnia 7 października 1999 r. o języku polskim (Dz. U. z 2011 r., Nr 43, poz. 224 z późn. zm) Zamawiający w opisie przedmiotu zamówienia użył terminologii angielskiej do pomocniczego określenia zakresu szkoleń - mimo że postępowanie w przedmiocie udzielenia zamówienia prowadzi się w języku polskim.
   Zamawiający wymaga, aby szkolenia były prowadzone w języku polskim lub angielskim.

   Zgodnie z art. 30 ustawy Pzp, Zamawiający **dopuszcza** możliwość zaoferowania rozwiązania **równoważnego. Wskazanie równoważności oferowanego przedmiotu zamówienia**

spoczywa na Wykonawcy. W przypadku zaproponowania rozwiązania równoważnego, Wykonawca dołączy do oferty dokładny opis umożliwiający jego porównanie z wymaganiami określonymi przez Zamawiającego. W przypadku szkoleń certyfikowanych Zamawiający wymaga, aby szkolenie równoważne posiadało akredytację oficjalnego akredytora wymaganego szkolenia.

Za równoważne, Zamawiający uzna szkolenia obejmujące, co najmniej przedmiot zawarty w szkoleniach o minimalnie takiej samej tematyce przedmiotowych szkoleń, taki samym minimalnym czasie wymagany do ich przeprowadzenia. Zamawiający wymaga również aby szkolenia równoważne posiadały odpowiednią akredytację, zgodnie z wymaganiami SIWZ (dla tych szkoleń dla których była przewidziana akredytacja).

3. Każdy z uczestników poszczególnych szkoleń otrzyma certyfikat.
4. Szkolenia odbywać się mogą na terenie Polski, Unii Europejskiej lub Stanów Zjednoczonych.
5. Wykonawca zobowiązany jest wliczyć w cenę vouchera:
   a) materiały szkoleniowe (wydruki slajdów, instrukcji do przeprowadzenia warsztatów, niezbędne licencjonowane oprogramowanie, jeżeli takie będzie konieczne), a w przypadku szkoleń akredytowanych – wszystkie materiały jakie są wymagane przez akredytora szkolenia;
   b) pomieszczenie szkoleniowe z wyposażeniem (projektor, stoły, krzesła, notesy, materiały do notowania) napoje ciepłe i zimne podczas przerw;
   c) w przypadku szkoleń, które będą odbywać się poza granicami Polski, transport samolotowy z lotnisk Warszawa Okęcie lub Warszawa Modlin do lotnisk położonych w kraju szkolenia (do 200 km od miejsca szkolenia);
   d) w przypadku szkoleń, które będą odbywać się poza granicami Polski, pobyt w hotelu minimum dwugwiazdkowym;
   e) Zamawiający wymaga, aby minimum 60 % szkoleń, które odbywać się będą na terenie Polski, realizowane były w Warszawie lub do 100 km od centrum Warszawy;
   f) Wykonawca powinien dążyć do zapewnienia szkoleń na terytorium Polski, z jednoczesnym zapewnieniem zapisu lit e);
   g) Jeżeli szkolenie nie jest możliwe do wykonania na terenie Polski, Wykonawca powinien dążyć do realizacji szkolenia na terenie Unii Europejskiej, a w ostateczności na terenie USA.
6. Zamawiający dopuszcza powierzenie zamówienia podwykonawcom. W takim przypadku Wykonawca ma obowiązek (zgodnie z art. 36b ustawy Pzp) wskazać w ofercie części zamówienia, których wykonanie Wykonawca zamierza powierzyć podwykonawcom,

IV. TERMIN WYKONANIA ZAMÓWIENIA

1. Wymagany okres realizacji zamówienia: **dostawa voucher'ów maksymalnie do 16.12.2015 r.**
2. Szkolenia odbywać się będą w terminach uzgodnionych z Zamawiającym, w okresie do 12 miesięcy od dnia podpisania umowy.

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

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki udziału w postępowaniu, w szczególności dotyczące:
   a) Posiadania uprawnień do wykonania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania:
   Zamawiający nie wyznacza szczegółowego warunku w tym zakresie, ocena spełnienia tego warunku dokonana zostanie na podstawie złożonego oświadczenia o spełnianiu warunku udziału w postępowaniu zgodnie z art. 22 ust. 1 ustawy Pzp.

b) Posiadania wiedzy i doświadczenia:
Zamawiający uzna spełnienie warunku określonego w pkt. b) jeżeli Wykonawca:
w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie: wykonał, co najmniej 3 usługi szkoleniowe lub dostawę voucherów szkoleniowych o wartości min. **100 000 zł brutto każda**, oraz załączy dokumenty potwierdzające, że roboty te zostały wykonane lub są wykonywane należycie.
Podstawowymi dowodami są:
- poświadczenia pochodzące od wystawcy dokumentu określające prawidłowość wykonanych prac z tym, że w odniesieniu do nadal wykonywanych robót okresowych lub ciągłych poświadczenie powinno być wydane nie wcześniej niż na 3 miesiące przed upływem terminu składania ofert;
- jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać poświadczenia, może złożyć oświadczenie o należytym wykonaniu robót.

c) Dysponowania odpowiednim potencjałem technicznym:
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie, ocena spełnienia tego warunku dokonana zostanie na podstawie złożonego oświadczenia o spełnianiu warunku udziału w postępowaniu zgodnie z art. 22 ust. 1 ustawy Pzp.

d) Dysponowania osobami zdolnymi do wykonania zamówienia:
Zamawiający uzna spełnienie warunku określonego, w pkt. d) jeżeli Wykonawca wykaże, że dysponuje lub będzie dysponował na czas realizacji zamówienia osobami zdolnymi wykonać zamówienie, tj. posiadającymi następujące doświadczenie i kwalifikacje:

- co najmniej jednym ekspertem ds. metodyki i procesu nauczania, który posiada:
  (1) wykształcenie wyższe;
  (2) minimum 3 letnie doświadczenie zawodowe związane z prowadzeniem zajęć i szkoleń w zakresie systemów teleinformatycznych;
  (3) minimum 500 godzin przeprowadzonych i udokumentowanych szkoleń/kursów.

e) Sytuacji ekonomicznej i finansowej:
Zamawiający nie wyznacza szczegółowego warunku w tym zakresie, ocena spełnienia tego warunku dokonana zostanie na podstawie złożonego oświadczenia o spełnianiu warunku udziału w postępowaniu zgodnie z art. 22 ust. 1 ustawy Pzp.

2. W postępowaniu mogą wziąć udział Wykonawcy, którzy wykażą się zdolnością do należytego wykonania zamówienia, o której mowa w art. 22 ust.5 ustawy Pzp.
3. Zgodnie z art. 26 ust. 2b ustawy Prawo zamówień publicznych, Wykonawca wykazując spełnianie warunków, o których mowa w art. 22 ust. 1 ustawy Pzp może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami w trakcie realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie (**w formie oryginału**) tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia **– zał. Nr 4 do SIWZ**.
Odwołanie się do zasobów innych podmiotów jest dopuszczalne pod warunkiem, że Wykonawca będzie dysponował tymi zasobami przy realizacji zamówienia.

Nie jest dopuszczalne posługiwanie się w toku postępowania o udzielenie zamówienia publicznego w celu wykazania spełniania warunków wiedzy i doświadczenia dokumentami podmiotu trzeciego, jeżeli podmiot ten nie będzie brał udziału w wykonaniu zamówienia.

4. Jeżeli Wykonawca, polega na zasobach innych podmiotów na zasadach określonych w art. 26 ust. 2b ustawy, a podmioty te będą brały udział w realizacji części zamówienia, Zamawiający żąda od Wykonawcy przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w pkt VI. 4 lit. a) i b) SIWZ.
5. Podmiot, który zobowiązał się do udostępnienia zasobów zgodnie z pkt. 3, odpowiada solidarnie z Wykonawcą za szkodę Zamawiającego powstałą wskutek nieudostępnienia tych zasobów, chyba że za nieudostępnienie zasobów nie ponosi winy.
6. W postępowaniu mogą wziąć udział Wykonawcy, którzy spełniają warunek udziału w postępowaniu dotyczący braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego w okolicznościach, o których mowa w art. 24 ust. 1 ustawy Pzp.
7. W postępowaniu mogą wziąć udział Wykonawcy, którzy spełniają warunek udziału w postępowaniu dotyczący braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego w okolicznościach, o których mowa w art. 24 ust. 2 pkt 5 ustawy Pzp.
8. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający będzie oceniał spełnienie warunków udziału w postępowaniu określonych w art. 22 ust. 1 ustawy Pzp łącznie. Warunek posiadania wiedzy i doświadczenia oraz dysponowania osobami zdolnymi do wykonania zamówienia zostanie spełniony gdy przynajmniej jeden Wykonawca wykaże, że posiada odpowiednie doświadczenie lub że dysponuje ww. osobami. W przypadku gdy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia nie spełniają ww. warunków, mogą polegać na doświadczeniu podmiotów trzecich z zaznaczeniem, że podmiot trzeci musi spełniać warunki określone w poniższej SIWZ - określone w rozdz. V ust.1 pkt. b i d (tj., że zrealizował 3 usługi szkoleniowe lub dostawę voucherów szkoleniowych o wartości min. **100 000 zł brutto każda**, oraz załączy dokumenty potwierdzające, że roboty te zostały wykonane lub są wykonywane należycie i/lub dysponuje lub będzie dysponował na czas realizacji zamówienia osobami zdolnymi wykonać zamówienie .
9. każdy z warunków określonych w pkt. 1 winien spełniać, co najmniej jeden z tych Wykonawców albo wszyscy ci Wykonawcy wspólnie.
10. Ocena spełnienia wyżej opisanych warunków udziału w postępowaniu będzie dokonywana na podstawie złożonych przez Wykonawcę w niniejszym postępowaniu dokumentów oraz oświadczeń.
11. Oferta Wykonawcy wykluczonego zostanie uznana za odrzuconą.
12. O wykluczeniu z postępowania oraz odrzuceniu oferty Wykonawcy zostaną zawiadomieni niezwłocznie po dokonaniu wyboru najkorzystniejszej oferty. Zawiadomienie zawierać będzie uzasadnienie faktyczne i prawne.

VI. WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

1. W celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy Pzp, do oferty należy załączyć:
   a) oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu określonych w art. 22 ust. 1 ustawy Pzp, **wzór zał. Nr 2 do SIWZ** (oryginał),
   b) Wykaz usług, z co najmniej 3 usługami szkoleniowymi lub dostawami voucherów szkoleniowych o wartości min. **100 000 zł brutto każda**, wraz z podaniem ich rodzaju i wartości, daty i miejsca wykonania oraz z załączeniem dowodów, określających, czy usługi te zostały wykonane lub są wykonywane w sposób należyty w okresie ostatnich trzech lat przed

upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – **wzór zał**. **Nr 6 do SIWZ;**

c) wykaz osób, które będą uczestniczyć w wykonaniu zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnego do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności, oraz informacją o podstawie do dysponowania tymi osobami - **wzór zał**. **Nr 7 do SIWZ**;

d) oświadczenie Wykonawcy, że osoby, które będą uczestniczyć w wykonywaniu zamówienia, posiadają wymagane uprawnienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień - **wzór zał**. **Nr 8 do SIWZ**.

e) **Pisemne zobowiązanie** innych podmiotów do oddania Wykonawcy do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia (jeżeli **Wykonawca składający ofertę będzie korzystał z zasobów innych podmiotów**), z treści którego wynikać powinno: zakres dostępnych Wykonawcy zasobów innego podmiotu, sposób wykorzystania zasobów innego podmiotu przy wykonywaniu zamówienia, charakter stosunku, jaki będzie łączył Wykonawcę z innym podmiotem, zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia - **wzór zał. Nr 4 do SIWZ.**

2. W przypadku wykazania w załączniku, o którym mowa w pkt. 1 b) niniejszej specyfikacji, w kolumnie wartość, rozliczeń w walutach obcych, Zamawiający dla wyliczenia ceny wykazanej roboty przeliczy walutę obcą według kursu sprzedaży waluty ogłoszonego w Tabeli kursów kupna i sprzedaży walut obcych NBP z dnia otwarcia ofert, zamieszczonego na stronie internetowej http://www.nbp.pl/Kursy/KursyC.html.
3. W przypadku oferty składanej przez Wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego, oświadczenie o spełnianiu każdego z warunków, o których mowa w art. 22 ust. 1 składa, co najmniej jeden z tych Wykonawców albo wszyscy ci Wykonawcy wspólnie.
4. W celu wykazania braku podstaw do wykluczenia z postępowania o udzielenie zamówienia z art. 24 ust. 1 ustawy Pzp Wykonawca składa następujące dokumenty:
   a) oświadczenie o braku podstaw do wykluczenia z postępowania z powodu niespełnienia warunków, o których mowa w art. 24 ust. 1 ustawy Pzp, **wzór zał. Nr 3 do SIWZ**,
   b) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust.1 pkt. 2 Ustawy Pzp, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
   c) Jeżeli Wykonawcy należą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. Nr 50, poz. 331, z późn. zm.) – nie mogą złożyć odrębnych ofert, chyba, że wykażą, że istniejące między nimi powiązania nie prowadzą do zachwiania uczciwej konkurencji pomiędzy Wykonawcami w postępowaniu o udzielenie zamówienia.
   W związku z powyższym Wykonawca składa listę podmiotów należących do tej samej grupy kapitałowej albo informację o tym, że nie należy do grupy kapitałowej – **wzór zał**. **Nr 5 do SIWZ.**
5. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczpospolitej Polskiej, zamiast dokumentów, o których mowa w pkt 4 b) składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio:
   a) nie otwarto jego likwidacji ani nie ogłoszono upadłości,
   Jeżeli w kraju miejsca zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa powyżej, zastępuje się dokumentem zawierającym oświadczenie, w którym określa się także osoby uprawnione do reprezentacji Wykonawcy złożone przed właściwym organem sądowym, administracyjnym albo

organem samorządu zawodowego lub gospodarczego odpowiednio kraju miejsca zamieszkania osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, lub przed notariuszem.

VII. INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIU OŚWIADCZEŃ LUB DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1. Niniejsze postępowanie jest prowadzone w języku polskim.
2. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
3. W postępowaniu o udzielenie zamówienia oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują:
   a) pisemnie na adres:

   Wojskowy Instytut Łączności
   ul. Warszawska 22 A
   05-130 Zegrze Południowe

   b) faksem na numer: 261 885 589
   c) droga elektroniczną: kancelaria@wil.waw.pl
4. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje faxem lub drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
5. W przypadku braku potwierdzenia otrzymania wiadomości przez Wykonawcę, Zamawiający domniema, iż pismo wysłane przez Zamawiającego na numer faksu lub drogą elektroniczną podane przez Wykonawcę zostało mu doręczone w sposób umożliwiający zapoznanie się Wykonawcy z treścią pisma.
6. W przypadku wezwania Wykonawcy na podstawie art. 26 ust.4 ustawy, do złożenia wyjaśnień dotyczących oświadczeń lub dokumentów, o których mowa w art. 25 ust. 1 Ustawy Pzp lub na podstawie art. 87 ust. 1 Ustawy Pzp do złożenia wyjaśnień dotyczących złożonej oferty, obowiązuje forma pisemna tzn. dokument należy złożyć w formie oryginału.
7. Zamawiający nie przewiduje udzielania żadnych ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane zapytania w sprawach wymagających zachowania pisemności postępowania.
8. W sprawie procedury przetargowej należy porozumiewać się z p. Katarzyną Juras oraz p. Agnieszką Zawadą.
9. W sprawie dotyczącej przedmiotu zamówienia należy porozumiewać się z p. Joanną Śliwą oraz z p. Bartoszem Jasiulem.

VIII. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ TREŚCI SIWZ

1. Wykonawca może zwrócić się do Zamawiającego z pisemną prośbą – wnioskiem o wyjaśnienie treści SIWZ. Zamawiający odpowie niezwłocznie, nie później jednak niż 2 dni przed upływem terminu składania ofert, na piśmie na zadane pytanie, przesyłając treść pytań i odpowiedzi wszystkim uczestnikom postępowania oraz umieści taką informacje na własnej stronie internetowej, pod warunkiem, że wniosek o wyjaśnienie treści specyfikacji wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

2. W przypadku rozbieżności pomiędzy treścią niniejszej specyfikacji a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze wyjaśnienia Zamawiającego.
3. Zamawiający nie przewiduje zwołania zebrania wszystkich Wykonawców w celu wyjaśnienia treści SIWZ.
4. Jeżeli w wyniku zmiany treści SIWZ nieprowadzącej do zmiany ogłoszenia o zamówieniu, niezbędny będzie dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert i poinformuje o tym Wykonawców, którym przekazano SIWZ oraz umieści taką informacje na własnej stronie internetowej.

IX. TERMIN ZWIĄZANIA OFERTĄ

1. Ustala się, że składający ofertę pozostaje nią związany przez 30 dni. Bieg tego terminu rozpoczyna się wraz z upływem terminu składania ofert.
2. Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

X. WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający nie wymaga w przedmiotowym postępowaniu wniesienia wadium**.**

XI. OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Oferta musi być sporządzona z zachowaniem formy pisemnej pod rygorem nieważności.
2. Oferta wraz z załącznikami musi być czytelna.
3. Oferta wraz z załącznikami musi być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy zgodnie z przedstawionym dokumentem, z którego wynika umocowanie prawne osoby podpisującej ofertę (odpis z KRS lub wyciąg z rejestru).
4. Podpisy Wykonawcy na oświadczeniach i dokumentach muszą być złożone w sposób pozwalający zidentyfikować osobę podpisującą. Zaleca się opatrzenie podpisu pieczątką z imieniem i nazwiskiem osoby podpisującej.
5. Pełnomocnictwo winno być w formie oryginału podpisanego przez osobę(y) upełnomocniającą(e) (pieczątka imienna oraz podpis lub pieczątka firmowa i czytelny podpis). Kserokopię dopuszcza się tylko w przypadku pełnomocnictwa udzielonego notarialnie. Złożenie kopii pełnomocnictwa notarialnego poświadczonego samodzielnie przez pełnomocnika nie jest wystarczające i skutkuje **wezwaniem do uzupełnienia**. Zgodnie z przepisami pełnomocnik do odwołania winien przedłożyć pełnomocnictwo z podpisem mocodawcy (oryginał) lub wierzytelny odpis pełnomocnictwa (poświadczoną za zgodność z oryginałem kopię) - art. 89 Kpc. Poświadczenie za zgodność odpisu z oryginałem dokonuje notariusz (art. 96 pkt 2 ustawy Prawo o notariacie).
6. Oferta wraz z załącznikami musi być sporządzona w języku polskim. Każdy dokument składający się na ofertę sporządzony w innym języku niż język polski winien być złożony wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę. W razie wątpliwości uznaje się, iż wersja polskojęzyczna jest wersją wiążącą.
7. Dokumenty mogą być przedstawiane w formie oryginałów (ew. notarialnie poświadczonej kserokopii) lub kserokopii poświadczonej **za zgodność z oryginałem** przez Wykonawcę, zgodnie z zasadami reprezentacji określonymi w dokumencie rejestrowym, lub przez upoważnionego przedstawiciela Wykonawcy. Każda zapisana strona przedstawiająca niezbędną dla spełnienia warunków zamówienia stawianych przez Zamawiającego treść winna być opatrzona: **czytelnym podpisem lub imienną pieczątką i podpisem.** W przypadku, gdy przedstawiona kserokopia dokumentu jest nieczytelna lub budzi wątpliwości, co do jego prawdziwości, a Zamawiający nie

może sprawdzić jej prawdziwości w inny sposób, może on żądać przedstawienia oryginału lub notarialnie potwierdzonej kopii dokumentu.

8. Zaleca się, by każda zawierająca jakąkolwiek treść strona oferty była podpisana lub parafowana przez Wykonawcę. Każda poprawka w treści oferty, a w szczególności każde przerobienie, przekreślenie, uzupełnienie, nadpisanie etc. powinny być parafowane przez Wykonawcę.
9. Zaleca się, aby strony oferty były trwale ze sobą połączone i kolejno ponumerowane. W treści oferty winna być umieszczona informacja o ilości stron.
10. W przypadku, gdy informacje zawarte w ofercie stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji, co do których Wykonawca zastrzega, że nie mogą być udostępnianie innym uczestnikom postępowania, muszą być oznaczone klauzulą: „Informacja stanowiąca tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. nr 153 poz. 1503)" i dołączone do oferty, zaleca się, aby były trwale, oddzielnie spięte.
11. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
12. Złożenie więcej niż jednej oferty zawierającej propozycje alternatywne spowoduje odrzucenie wszystkich ofert złożonych przez Wykonawcę.
13. Wykonawca wskaże w ofercie tę część zamówienia, której wykonanie powierzy Podwykonawcom.
14. Na ofertę składają się:
    a) formularz oferty (**zał. Nr 1 do SIWZ**). Załącznik należy wypełnić we wszystkich wymaganych (pustych) miejscach,
    b) oświadczenie Wykonawcy o spełnianiu warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy Pzp, wg załączonego wzoru (**zał. Nr 2 do SIWZ**),
    c) oświadczenie Wykonawcy o spełnianiu warunku udziału w postępowaniu, dotyczącym braku podstaw do wykluczenia, o których mowa w art. 24 ust. 1 ustawy Pzp (**zał. Nr 3 do SIWZ**.),
    d) wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, usług (lub dostaw), w okresie ostatnich trzech lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których zamówienia zostały wykonane oraz załączeniem dowodów, czy zostały wykonane lub są wykonywane należycie (**zał. Nr 6 do SIWZ**),
    e) wykaz osób, które będą uczestniczyć w wykonaniu zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnego do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności, oraz informacją o podstawie do dysponowania tymi osobami. (**zał. Nr 7 do SIWZ**),
    f) lista podmiotów należących do tej samej grupy kapitałowej, co Wykonawca albo informacja o tym, że Wykonawca nie należy do tej samej grupy kapitałowej (**zał. Nr 5 do SIWZ**),
    g) oświadczenie Wykonawcy, że osoby, które będą uczestniczyć w wykonywaniu zamówienia, posiadają wymagane uprawnienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień (**zał. Nr 8 do SIWZ**),
    h) aktualny odpis z właściwego rejestru, jeżeli odrębne przepisy wymagają wpisu do rejestru, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy Pzp,
    i) **pisemne zobowiązanie** innych podmiotów do oddania Wykonawcy do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia - jeżeli **Wykonawca składający ofertę będzie korzystał z zasobów innych podmiotów**, (**zał. Nr 4 do SIWZ),**
    j) **opis przedmiotu zamówienia, który stanowi formularz cenowy – z opisem zaoferowanych rozwiązań równoważnych, (zał. nr 10 do SIWZ).**
    k) pełnomocnictwo do reprezentowania Wykonawcy, o ile ofertę składa pełnomocnik.

XII. MIEJSCE ORAZ TERMIN SKŁADANIA OFERT

1. Oferty muszą być złożone w siedzibie Zamawiającego w Zegrzu Południowym przy ul. Warszawskiej 22A, Kancelaria Jawna, w terminie **do dnia 04.12.2015 r. do godziny 13:00.** Wjazd na teren WIŁ możliwy jest po wystawieniu przepustek.
2. Ofertę należy umieścić w zamkniętym opakowaniu, uniemożliwiającym odczytanie zawartości bez uszkodzenia tego opakowania. Opakowanie winno być oznaczone nazwą (firmą) i adresem Wykonawcy, zaadresowane na adres Zamawiającego oraz opisane: **„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych”**, **Nie otwierać przed 04.12.2015 r. godz. 13.15, nr postępowania ZP-13-15-CYBERSECLAB”.**
3. Oferta otrzymana przez Zamawiającego po terminie składania ofert zostanie niezwłocznie zwrócona Wykonawcy bez otwierania.
4. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu zmian musi być złożone według takich samych zasad, jak składana oferta tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA”. Koperty oznakowane „ZMIANA” zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.
5. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia. Powiadomienie o wycofaniu oferty powinno być opakowane i zaadresowane w ten sam sposób, co oferta. Dodatkowo opakowanie, w którym jest przekazywane powiadomienie należy opatrzyć napisem „WYCOFANIE”.

XIII. MIEJSCE ORAZ TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w siedzibie Zamawiającego przy ul. Warszawskiej 22A w Zegrzu Południowym w sali nr 101, **w dn. 04.12.2015 r. o godz. 13:15**
2. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
3. Podczas otwarcia ofert Zamawiający poda nazwy (firmy), adresy Wykonawców, informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.
4. Otwarcie ofert jest jawne, Wykonawcy mogą uczestniczyć w sesji otwarcia ofert. W przypadku nieobecności Wykonawcy przy otwieraniu ofert, Zamawiający prześle na pisemny wniosek Wykonawcy informację z otwarcia ofert.

XIV. OPIS SPOSOBU OBLICZENIA CENY

1. Cena ofertowa powinna obejmować wszystkie koszty i składniki związane z wykonaniem zamówienia, uwzględniająca cały zakres przedmiotu zamówienia, oraz ewentualne ryzyko wynikające z okoliczności, które można było przewidzieć w terminie opracowywania oferty do czasu jej złożenia.
2. W „Formularzu ofertowym” należy podać w PLN cenę netto, stawkę podatku VAT wartość VAT oraz cenę brutto (cyfrowo i słownie).
3. Stawkę podatku VAT należy określić według obowiązujących przepisów i stanu faktycznego na dzień złożenia oferty.
4. Zamawiający nie przewiduje rozliczenia w walutach obcych kraju Wykonawcy składającego ofertę.
5. W przypadku Wykonawców wspólnie ubiegających się o zamówienia rozliczenia dokonywane będą z ich pełnomocnikiem.

6. Jeżeli w przedmiotowym postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania oraz wskazując ich wartość bez kwoty podatku.
7. W przypadku, o którym mowa w ust. 7, jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, do ceny najkorzystniejszej oferty lub oferty z najniższą ceną dolicza się podatek od towarów i usług, który Zamawiający miałby obowiązek rozliczyć zgodnie z tymi przepisami.

XV. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami i ich znaczeniem:
   a) Cena ofertowa: **80 pkt.**
   b) Dostarczenie spersonalizowanego dostępu do zasobów on-line, kursów i ścieżek certyfikacyjnych, publikacji oraz filmów instruktażowych dla min. 7 osób na okres 12 miesięcy od dnia ich dostarczenia (dostawa odbyć się powinna maksymalnie w ciągu pięciu dni od dnia podpisania umowy): **20 pkt.**

W ramach kryterium określonego w pkt.b) Zamawiający wymaga:

- spersonalizowanego dostępu do zasobów on line, kursów i ścieżek certyfikacyjnych, publikacji oraz filmów instruktażowych dla min. 7 osób. Uczestnik po otrzymaniu loginów i hasła do bazy wiedzy, będzie posiadał do niego nieograniczony dostęp przez 12 miesięcy od dnia ich dostarczenia (dostawa odbyć się powinna maksymalnie w ciągu pięciu dni kalendarzowych od dnia podpisania umowy). Zakres tematyczny zasobów on-line powinien obejmować minimum takie zagadnienia jak:

a) Bezpieczeństwo
b) Akredytacje w zakresie bezpieczeństwa
c) Cyber Bezpieczeństwo
d) Audytowanie
e) Bezpieczeństwo w procesie tworzenia oprogramowania
f) Bezpieczeństwo sieci
g) Kryptografia
h) Informatyka śledcza
i) Systemy operacyjne i technologie serwerowe
j) Technologie sieciowe
k) Systemy internetowe
l) Bazy danych
m) Software Development
n) Systemy ERP
o) Zarządzanie projektami

- Zasoby wiedzy powinny być opatrzone elementami sprawdzającymi wiedzę, wraz z możliwością uzyskania jak najwyższej punktacji. Dostawca powinien zagwarantować zgodność materiału sprawdzającego wiedzę z oczekiwaniami jednostek certyfikujących, odpowiednio w każdym z działów tematycznych.

- Zasoby wiedzy powinny być dostarczone wraz z narzędziem niezbędnym do uruchomienia, korzystania i monitorowania przyrostu wiedzy i kompetencji uczestników szkoleń.
- Dostawca zobowiązany jest to przekazania loginów najpóźniej 5 dni kalendarzowych od podpisania umowy.

2. Maksymalna ilość punktów, jaką Wykonawca może uzyskać przy ocenie, wynosi łącznie 100 pkt.

3. Zasady oceny ofert:
   a) wartość punktowa oferty wg. kryterium ceny obliczona będzie przy pomocy wzoru:

$$C = (\frac{Nco}{Cob}) \times 80\, pkt$$

   Nco – najniższa cena spośród wszystkich ofert,

   Cob – cena oferty badanej.

   b) wartość punktowa oferty wg kryterium: Dostarczenia spersonalizowanego dostępu do zasobów on-line, kursów i ścieżek certyfikacyjnych, publikacji oraz filmów instruktażowych dla min. 7 osób na okres min. 12 miesięcy od dnia dostarczenia (dostawa odbyć się powinna maksymalnie w ciągu pięciu kalendarzowych dni od dnia podpisania umowy) – **20** pkt.

   Wykonawca, który nie zaproponuje powyższej opcji otrzyma - **0** pkt.

4. W oparciu o powyższe kryteria opisane wzorami zostanie sporządzone zbiorcze zestawienie oceny ofert. Punkty będą liczone z dokładnością do dwóch cyfr po przecinku.
5. Zamawiający uzna za najkorzystniejszą tę ofertę (spośród niepodlegających odrzuceniu), która uzyska najwyższą łączną liczbę punktów w ramach poszczególnych, wyżej wymienionych, kryteriów oceny ofert.
6. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom przedstawionym w ustawie – Prawo zamówień publicznych oraz SIWZ i została oceniona, jako najkorzystniejsza w oparciu o podane powyżej kryteria wyboru.

XVI. UDZIELENIE ZAMÓWIENIA

1. Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w Ustawie Pzp oraz w niniejszej specyfikacji i zostanie oceniona, jako najkorzystniejsza w oparciu o podane w ogłoszeniu i SIWZ kryteria wyboru.
2. O odrzuceniu ofert/y oraz wyborze najkorzystniejszej oferty, Zamawiający zawiadomi niezwłocznie Wykonawców, którzy złożyli oferty w przedmiotowym postępowaniu, podając uzasadnienie faktyczne i prawne.
3. Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający zamieści informacje, określone w art. 92 ust. 1 pkt 1 Ustawy Pzp na własnej stronie internetowej oraz w swojej siedzibie.
4. Zamawiający zawrze umowę w sprawie zamówienia publicznego w terminie nie krótszym niż 5 dni od dnia przekazania zawiadomienia o wyborze oferty faksem.
5. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem 5-dniowego terminu, jeżeli w postępowaniu zostanie złożona tylko jedna oferta.

XVII. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. W przypadku udzielenia zamówienia konsorcjum (tzn. Wykonawcy określonemu w art. 23 ust. 1 Ustawy Pzp), Zamawiający przed podpisaniem umowy zażąda złożenia umowy regulującej współpracę tych Wykonawców.
2. Przed podpisaniem umowy Zamawiający może poprosić Wykonawcę o przedstawienie dokumentów potwierdzających posiadanie przez osoby przedstawione w Wykazie osób, stosownych uprawnień (tj. w specjalności sanitarnej) jak również aktualnego zaświadczenia o przynależności danej osoby do właściwej Izby Samorządu Zawodowego. Powyższe dokumenty Wykonawca zobowiązany będzie dostarczyć w formie oryginału lub kopii poświadczonej „za zgodność z oryginałem".
3. Zamawiający wymaga wniesienia zabezpieczenia należytego wykonania umowy zgodnie z zapisami projektu umowy stanowiącego załącznik nr 9 do SIWZ.

XVIII. ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWENIA PUBLICZNEGO

1. Wzór umowy znajduje się **w zał. Nr 9 do SIWZ**.
2. Zamawiający przewiduje zmiany w umowie dotyczące przedmiotu zamówienia w następujących przypadkach:
   a) zmiany obowiązujących przepisów prawa,
   b) uzasadnionych przyczyn technicznych lub funkcjonalnych powodujących konieczność zmiany sposobu wykonania umowy,
   c) jeżeli zmiana jest korzystna dla Zamawiającego,
   d) w sytuacji wystąpienia problemów finansowych po stronie Zamawiającego z przyczyn od niego niezależnych. Zmiana postanowień umowy może dotyczyć m.in. zmiany zakresu przedmiotu umowy, wynagrodzenia, terminu realizacji itp. w takiej sytuacji zmianie ulegnie umowa w zakresie koniecznym do jej prawidłowej realizacji i zostanie wprowadzona aneksem,
   e) w sytuacji wystąpienia zjawisk związanych z działaniem siły wyższej (jak np. klęska żywiołowa, niepokoje społeczne, działania militarne, pożar itp.) Zmiana postanowień umowy może dotyczyć m.in. zmiany zakresu przedmiotu umowy, wynagrodzenia, terminu realizacji itp. W takiej sytuacji zmianie ulegnie umowa w zakresie koniecznym do prawidłowej realizacji i zostanie wprowadzona aneksem. Nie uważa się za czynnik zakłócający wpływ czynników atmosferycznych w czasie realizacji robót, który musi być normalnie brany pod uwagę (wyjątek stanowią przeszkody atmosferyczne o charakterze katastrof).
   f) zmiany osób odpowiedzialnych za realizację zamówienia, zarówno ze strony Zamawiającego, jak i Wykonawcy, zmiana danych teleadresowych, zmiany osób reprezentujących strony itp. podobne zmiany nie stanowią istotnej zmiany umowy w rozumieniu art. 144 ustawy Pzp,
3. Nie stanowi istotnej zmiany umowy w rozumieniu art. 144 ust. 1 ustawy Pzp:
   a) zmiana danych związanych z obsługą administracyjno-organizacyjną umowy (np. zmiana nr rachunku bankowego),
   b) zmiana danych teleadresowych,
   c) zmiana osób wskazanych do kontaktów między stronami.
4. Warunkiem dokonania zmian, o których mowa w pkt. 2 b), c) i e) jest złożenie wniosku przez Stronę inicjującą zmianę zawierającego:
   a) opis propozycji zmiany,
   b) uzasadnienie zmiany,
   c) obliczenie kosztów zmiany zgodnie z zasadami określonymi w Umowie, jeżeli zmiana będzie miała wpływ na wynagrodzenie Wykonawcy,
   d) opis wpływu zmiany na termin wykonania Umowy.
5. Zmiany, o których mowa w pkt. 2 b) mogą zostać dokonane, jeżeli zachodzi i jest jej uzasadnieniem co najmniej jedna z niżej wymienionych okoliczności:

a) poprawa jakości,
b) zmiany obowiązujących przepisów lub obowiązek dostosowania do obowiązujących przepisów.

6. Ponadto zmiany, o których mowa w pkt. 2 mogą dotyczyć:
   a) ustawowej zmiany stawki podatku VAT,
8. Zmiana umownego terminu zakończenia realizacji przedmiotu umowy możliwa jest w następujących przypadkach:
   a) w skutek działania siły wyższej.
10. Wyżej wskazane zmiany zostaną wprowadzone w postaci aneksu do umowy w sprawie zamówienia publicznego w przypadku zaistnienia zdarzeń wymienionych w pkt. 2. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.

XIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

Środki ochrony prawnej opisane w dziale VI Ustawy Pzp przysługują Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy.

XX. INFORMACJE DODATKOWE

1. Zamawiający nie przewiduje udzielenia zamówień uzupełniających.
2. Zamawiający nie przewiduje zawarcia umowy ramowej.
3. Zamawiający nie przewiduje ustanowienia dynamicznego systemu zakupów oraz wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.
4. Zamawiający nie dopuszcza prowadzenia rozliczeń w obcych walutach.
5. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
6. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

XXI. ZAŁĄCZNIKI

1. Formularz ofertowy.
2. Oświadczenie o spełnianiu warunków udziału w postępowaniu.
3. Oświadczenie o braku podstaw do wykluczenia.
4. Zobowiązanie innych podmiotów.
5. Informacja o przynależności do grupy kapitałowej.
6. Wykaz wykonanych robót budowlanych.
7. Wykaz osób, które będą uczestniczyć w wykonaniu zamówienia.
8. Oświadczenie Wykonawcy potwierdzające posiadanie wymaganych uprawnień przez osoby uczestniczące w wykonaniu zamówienia.
9. Wzór umowy.
10. Opis przedmiotu zamówienia - formularz cenowy.
11. Wymagania na szkolenia dla CybrSecLab (pomocniczego określenia zakresu szkoleń).

Podpisy:

Przewodniczący	Krzysztof Łysek	…….
Sekretarz	Agnieszka Zawada	……..……
Członkowie:	Katarzyna Juras	……..……
	Joanna Śliwa	……..

Bartosz Jasiul ……..

Załącznik nr 1 do SIWZ

……
(pieczęć Wykonawcy)

Formularz ofertowy

Dane dotyczące Wykonawcy:

Nazwa: .....,

Siedziba: .....,

(nazwa i siedziba Wykonawcy - w przypadku wspólnego ubiegania się o udzielenie zamówienie należy wymienić wszystkich Wykonawców ze wskazaniem Pełnomocnika, a poniżej wpisać jedynie dane Pełnomocnika)

Nr telefonu/faksu: .....,

Internet: http:// .....,

e-mail: .....@.....,

REGON .....; NIP .....,

Osoby uprawnione do porozumiewania się z Zamawiającym:

.....

Zamawiający:

Wojskowy Instytut Łączności
ul. Warszawska 22A
05-130 Zegrze

W związku z postępowaniem prowadzonym w trybie przetargu nieograniczonego na wykonanie przedmiotu **„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych", nr sprawy ZP/13/15/CYBERSECLAB.**

1. Oferujemy wykonanie przedmiotu zamówienia określonego w SIWZ za kwotę:

Łączna wartość zamówienia:

netto: ..... *zł.* (słownie złotych: .....)

plus podatek VAT w wysokości .... %, co daje kwotę podatku: …… zł,

łącznie:

brutto: ..... *zł.* (słownie złotych: .....)

2. Oświadczamy, że*:*

a) **dostarczymy vouchery maksymalnie do ……..…… (nie później niż 16.12.2015 r.)** Szkolenia zrealizujemy w ciągu …… od dnia podpisania umowy (nie później niż w ciągu 12 miesięcy).

b) **Dostarczymy/ nie dostarczymy*** spersonalizowany dostęp do zasobów on-line, kursów i ścieżek certyfikacyjnych, publikacji oraz filmów instruktażowych dla min. 7 osób na okres 12 miesięcy od dnia dostarczenia (dostawa odbyć się powinna maksymalnie w ciągu pięciu dni kalendarzowych od dnia podpisania umowy).

c) Oświadczamy, że zamierzamy/nie zamierzamy* powierzyć wykonanie części zamówienia podwykonawcom w zakresie …….....

……

d) Oświadczamy, że polegamy na wiedzy i doświadczeniu*, potencjale technicznym*, osobach zdolnych do wykonania zamówienia* lub zdolnościach finansowych*, następujących podmiotów **które będą brały udział w realizacji części zamówienia** ……...

……*

e) Oświadczamy, że polegamy na wiedzy i doświadczeniu*, potencjale technicznym*, osobach zdolnych do wykonania zamówienia* lub zdolnościach finansowych*, następujących podmiotów **które nie będą brały udział w realizacji części zamówienia**……...

……*

f) zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia wraz z załącznikami, nie wnosimy do nich zastrzeżeń oraz zdobyliśmy konieczne informacje potrzebne do sporządzenia oferty i właściwego wykonania zamówienia;

g) załączone do oferty dokumenty opisują stan prawny i faktyczny, aktualny na dzień otwarcia ofert (odpowiedzialność karna na podstawie art. 233 kk);

h) kwota oferty zawiera wszystkie koszty związane z realizacją przedmiotu zamówienia, w tym koszt voucherów, szkoleń, transportu, noclegu dla osób będących uczestnikami szkoleń (jeśli takowe wystąpią) oraz należne cła i podatki;

i) akceptujemy określone przez Zamawiającego w projekcie umowy zasady płatności, tj. płatność przelewem w terminie 21 dni od daty otrzymania prawidłowo wystawionej faktury VAT;

j) zawarty w Specyfikacji Istotnych Warunków Zamówienia wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wybrania naszej oferty, do zawarcia umowy na wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego;

k) uważamy się za związanych niniejszą ofertą przez okres 30 dni licząc od dnia, w którym upływa termin składania ofert;

l) wyżej wskazany numer faksu i e-mail jest odpowiednim do przekazywania nam informacji dotyczących postępowania.

**** - niepotrzebne skreślić***

.....	.....
(miejscowość, data)	*(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)*

Załącznik nr 2 do SIWZ

Pieczęć adresowa Wykonawcy

.....

Oświadczenie o spełnieniu warunków udziału w postępowaniu

Ja niżej podpisany.....

reprezentujący Wykonawcę.....

będąc uczestnikiem postępowania o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego** organizowanego przez Wojskowy Instytut Łączności na:

„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych" nr sprawy ZP/13/15/CYBERSECLAB

Oświadczam, że zgodnie z art. 22 ust. 1 pkt 1- 4 ustawy Pzp spełniam warunki dotyczące:

1. Posiadania uprawnień do wykonywania określonej w Specyfikacji Istotnych Warunków Zamówienia oraz ofercie działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania.
2. Posiadania wiedzy i doświadczenia.
3. Dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia.
4. Sytuacji ekonomicznej i finansowej.

....

(miejscowość, data) *(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)*

Załącznik nr 3 do SIWZ

Pieczęć adresowa Wykonawcy

.....

Oświadczenie o braku podstaw do wykluczenia z postępowania

Ja niżej podpisany .....

reprezentujący Wykonawcę.....

będąc uczestnikiem postępowania o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego** organizowanego przez Wojskowy Instytut Łączności na:

„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych"

nr sprawy ZP/13/15/CYBERSECLAB

oświadczam, że **nie podlegam wykluczeniu** z postępowania o udzielenie zamówienia na podstawie **art. 24** ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz.U. z 2013r. poz. 907 z późn. zm.)

..... *(miejscowość, data)*

..... *(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)*

Załącznik nr 4 do SIWZ

Pieczęć adresowa Wykonawcy

.....

Z O B O W I Ą Z A N I E
innych podmiotów na podstawie art. 26 ust. 2 b ustawy

.....
(nazwa firmy lub imię i nazwisko)

.....
(siedziba firmy lub miejsce zamieszkania)

Tel.: ……. Faks: …….. e-mail: …….

W postępowaniu o udzielenie zamówienia publicznego organizowanego przez Wojskowy Instytut Łączności na: **„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych" nr sprawy ZP/13/15/CYBERSECLAB** – zobowiązuję się oddać do dyspozycji Wykonawcy:

……
(podać nazwę Wykonawcy, a w przypadku wspólnego ubiegania się o zamówienia – wszystkich Wykonawców składających wspólnie ofertę)

niezbędne zasoby:

1) wiedzę i doświadczenie*
2) potencjał techniczny*
3) osoby zdolne do wykonania zamówienia*
4) zdolności finansowe*

na zasadach: (opisać zakres dostępnych Wykonawcy zasobów innego podmiotu, sposób wykorzystania zasobów innego podmiotu przy wykonywaniu zamówienia, charakter stosunku, jaki będzie łączył wykonawcę z innym podmiotem, zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia) ……...
……
……
……

....., dnia.....r.

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

** - niepotrzebne skreślić*

Załącznik nr 5 do SIWZ

Pieczęć adresowa Wykonawcy

.....

Informacja z listą podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy, albo informację o tym, że nie należy do grupy kapitałowej

Przedmiot zamówienia: **„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych"**

nr sprawy ZP/13/15/CYBERSECLAB

Oświadczam, **że należę/nie należę*** do grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy.

Tabela. Lista podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5 ustawy **

Lp.	Nazwa podmiotu należącego z Wykonawcą do tej samej grupy kapitałowej	Uwagi
1.		
2.		
3.		
***		

* niepotrzebne skreślić,
** należy podać w przypadku przynależności do grupy kapitałowej o której mowa w art. 24 ust. 2 pkt 5 ustawy
*** w razie potrzeby dodać liczbę pozycji

.....
(miejscowość, data)

.....
(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik nr 6 do SIWZ

Pieczęć adresowa Wykonawcy

.....

WYKAZ WYKONANYCH W OKRESIE OSTATNICH TRZECH LAT USŁUG

Lp.	Odbiorca usługi: nazwa i adres, telefon	Przedmiot usługi odpowiadający przedmiotowi zamówienia	Termin wykonania (data rozpoczęcia i zakończenia) dd/mm/rrrr – dd/mm/rrrr	Wartość usługi z podatkiem VAT w zł
1	***2***	***3***	***5***	***6***

W załączeniu referencje lub inne dokumenty potwierdzające należyte wykonanie w ilości .....szt.

.....
(miejscowość, data)

…….....
(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik nr 7 do SIWZ

pieczęć adresowa firmy Wykonawcy

Wykaz osób, które będą uczestniczyć w wykonaniu zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczeniu i wykształceniu niezbędnym do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności oraz informacja o podstawie do dysponowania tymi osobami

Ja niżej podpisany .....

reprezentujący Wykonawcę.....

będąc uczestnikiem postępowania o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego,** organizowanego przez Wojskowy Instytut Łączności na:

„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych"

nr sprawy ZP/13/15/CYBERSECLAB

Poniżej przedstawiam, wykaz osób, które będą uczestniczyć w wykonaniu zamówienia.

l.p.	Imię i nazwisko	Informacja na temat kwalifikacji zawodowych	Doświadczenie i wykształcenie niezbędne do wykonania zamówienia	Zakres wykonywanych czynności	Informacja o podstawie do dysponowania osobą
1.					
2.					
3.					

.....
(miejscowość, data)

…….....
(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik nr 8 do SIWZ

pieczęć adresowa firmy Wykonawcy

OŚWIADCZENIE

Ja niżej podpisany .....

reprezentujący Wykonawcę.....

będąc uczestnikiem postępowania o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego** organizowanego przez Wojskowy Instytut Łączności na:

„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych"

nr sprawy ZP/13/15/CYBERSECLAB

Oświadczam, że osoby, które będą uczestniczyć w wykonywaniu zamówienia, posiadają wymagane uprawnienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień.

.....
(miejscowość, data)

…….....
(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

Załącznik nr 9

UMOWA NR .....(Projekt)

W dniu ..... w Zegrzu Południowym pomiędzy:

WOJSKOWYM INSTYTUTEM ŁĄCZNOŚCI z siedzibą w Zegrzu Płd. (05-130) ul. Warszawska 22A, zarejestrowanym w Sądzie Rejonowym dla m. st. Warszawy w Warszawie, XIV Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000160194, NIP 524-030-70-48, NIP EU PL5240307048, REGON 010099060, reprezentowanym przez:

.....,

zwanym w treści umowy Zamawiającym,

a firmą ..... z siedzibą w ....., ul ....., wpisaną do ....., pod numerem ....., NIP ....., REGON ....., reprezentowaną przez:

.....,

zwaną w treści umowy Wykonawcą,

łącznie zwani Stronami,

została zawarta umowa następującej treści:

§ 1.

Zamawiający oświadcza, że niniejsza umowa zostaje zawarta po przeprowadzeniu postępowania o udzielenie zamówienia publicznego na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2013 r. poz. 907 z późn. zm.) w trybie przetargu nieograniczonego, nr sprawy **ZP-13-15-CYBERSECLAB.**

Zamówienie jest współfinansowane ze środków Unii Europejskiej w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet 2. Infrastruktura sfery B+R, Działanie 2.3: Inwestycje związane z rozwojem infrastruktury informatycznej nauki, Poddziałanie 2.3.1 Projekty w zakresie rozwoju infrastruktury informatycznej nauki, Poddziałanie 2.3.2 Projekty w zakresie rozwoju zasobów informacyjnych nauki w postaci cyfrowej, Poddziałanie 2.3.3 Projekty w zakresie rozwoju zaawansowanych aplikacji i usług teleinformatycznych, Projekt Nr POIG 02.03.00-14-106/13.

„Szkolenia dla zespołu Laboratorium Analiz Ataków Cybernetycznych"

§ 2.

1. Przedmiotem umowy jest usługa **Szkoleń dla zespołu Laboratorium Analiz Ataków Cybernetycznych** zgodnie z załącznikiem nr 1 do umowy – Opis przedmiotu umowy –formularz cenowy.
2. W przypadku braku możliwości zorganizowania przez Wykonawcę któregokolwiek ze szkoleń objętych umową i wynikających z voucherów, Wykonawca może zaproponować inne szkolenie z tego zakresu po akceptacji przez Zamawiającego. Wartość tego szkolenie nie może być wyższa od szkolenia planowanego.
3. Każdy z uczestnik poszczególnych szkoleń otrzyma certyfikat.
4. Szkolenia odbywać się mogą na terenie Polski, Unii Europejskiej lub Stanów Zjednoczonych.
5. Cena vouchera zawiera:
   a) materiały szkoleniowe (wydruki slajdów, instrukcji do przeprowadzenia warsztatów, niezbędne licencjonowane oprogramowanie, jeżeli takie będzie konieczne), a w przypadku szkoleń akredytowanych – wszystkie materiały jakie są wymagane przez akredytora szkolenia;

b) pomieszczenie szkoleniowe z wyposażeniem (projektor, stoły, krzesła, notesy, materiały do notowania) napoje ciepłe i zimne podczas przerw;
c) w przypadku szkoleń, które będą odbywać się poza granicami Polski, transport samolotowy z lotnisk Warszawa Okęcie lub Warszawa Modlin do lotnisk położonych w kraju szkolenia (do 200 km od miejsca szkolenia);
d) w przypadku szkoleń, które będą odbywać się poza granicami Polski, pobyt w hotelu minimum dwugwiazdkowym;
e) Zamawiający wymaga, aby minimum 60 % szkoleń, które odbywać się będą na terenie Polski, realizowane były w Warszawie lub do 100 km od centrum Warszawy;
f) Wykonawca powinien dążyć do zapewnienia szkoleń na terytorium Polski, z jednoczesnym zapewnieniem zapisu lit e);
g) Jeżeli szkolenie nie jest możliwe do wykonania na terenie Polski, Wykonawca powinien dążyć do realizacji szkolenia na terenie Unii Europejskiej, a w ostateczności na terenie USA.

§ 3.

Umowa zostaje zawarta na okres od dnia podpisania umowy do dnia ……. (maks. 16.12.2015 r), tj. w tym terminie zostaną dostarczone do Zamawiającego vouchery na szkolenia. Szkolenia odbywać się będą w terminach uzgodnionych z Zamawiającym, w okresie do 12 miesięcy od dnia podpisania umowy

§ 4.

1. Wynagrodzenie Wykonawcy, z tytułu wykonania przedmiotu umowy określonego szczegółowo w **§ 1**, Strony ustalają na stałą i niezmienną kwotę w łącznej wysokości..... zł (słownie: ..... zł) + VAT zgodnie z obowiązującymi przepisami, co daje kwotę: brutto: ……zł (słownie złotych:……).
2. Zamawiający oświadcza, że przedmiotowe usługi szkoleniowe są finansowane w całości ze środków publicznych na podstawie art. 43 ust. 1 pkt. 29c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2011 r., Nr 177, poz. 1054 z późn. zm.) zwolnione są z podatku VAT.
3. Faktura Wykonawca wystawi fakturę VAT po dostarczeniu voucherów, po podpisaniu przez Zamawiającego bez zastrzeżeń protokołu odbioru voucherów.
4. Wynagrodzenie ryczałtowe za przedmiot umowy zostanie uregulowane na podstawie doręczonego Zamawiającemu oryginału faktury VAT. Zapłata nastąpi w formie przelewu bankowego na rachunek wskazany przez Wykonawcę w fakturze w terminie 21 dni od daty otrzymania prawidłowo wystawionej faktury VAT. Termin uważa się za dochowany, jeżeli obciążenie rachunku Zamawiającego nastąpi do ostatniego dnia terminu płatności.
5. **Faktura musi być wystawiona przez Wykonawcę do 18.12.2015**r.
6. Zamawiający oświadcza, że dokonał zgłoszenia rejestracyjnego i decyzją Urzędu Skarbowego otrzymał Numer Identyfikacji Podatkowej 524-030-70-48.
7. Wykonawca oświadcza, że dokonał zgłoszenia rejestracyjnego i decyzją Urzędu Skarbowego otrzymał Numer Identyfikacji Podatkowej .....

§ 5

1. Strony ustalają zabezpieczenie należytego wykonania umowy w wysokości 10% wartości przedmiotu umowy brutto tj. **..... zł** (słownie: ..... złotych), które to Wykonawca wniesie najpóźniej w dniu podpisania umowy.
2. Zabezpieczenie, o którym mowa w ust. 1, służy pokryciu ewentualnych roszczeń z tytułu niewykonania lub nienależytego wykonania umowy.
3. Zabezpieczenie będzie zwracane w terminie maksymalnie 75 dni od dnia wykorzystania vouchera szkoleniowego i uznania przez Zamawiającego, że szkolenie zostało przeprowadzone należycie.

Za termin wykorzystania vouchera uznaje się dzień zgłoszenia do Wykonawcy zapotrzebowania na jego realizację. Szkolenie w ramach vouchera powinno zostać zrealizowane w terminie 60 dni od dnia zgłoszenia przez Zamawiającego potrzeby jego wykorzystania.

4. Jeżeli Wykonawca jest jednocześnie gwarantem, zabezpieczenie będzie służyć także pokryciu roszczeń z tytułu gwarancji i rękojmi. Kwota pozostawiona na zabezpieczenie tych roszczeń stanowi 30% wysokości zabezpieczenia.
5. Zabezpieczenie, o którym mowa w ust. 1, może być wniesione wg wyboru Wykonawcy, w następujących formach:
   - Formie pieniężnej;
   - Poręczeniach bankowych;
   - Gwarancjach bankowych;
   - Gwarancjach ubezpieczeniowych.
   - Poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2007 r. Nr 42 poz. 275 z późn. zm.).
6. Jeżeli zabezpieczenie, o którym mowa w ust. 1, Wykonawca wniesie w formie pieniężnej, to wpłaca je przelewem na rachunek bankowy wskazany przez Zamawiającego, tj. **ING Bank Śląski S.A. nr 89 1050 1012 1000 0023 5787 1413.**
7. Zabezpieczenie wniesione w formie pieniężnej, Zamawiający przechowuje na oprocentowanym rachunku bankowym.
8. Zamawiający, jeżeli nie zachodzi przypadek wskazany w ust. 2, zwraca zabezpieczenie wniesione w formie pieniężnej z odsetkami, wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.
9. W trakcie realizacji umowy, Wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w ust.5, za zgodą Zamawiającego.
10. Zmiana formy zabezpieczenia może być dokonana z zachowaniem ciągłości zabezpieczenia i bez zmniejszania jego wysokości.
11. Zamawiający, w terminie 30 dni od dnia ostatecznego wykorzystania voucherów i uznania jej przez Zamawiającego za należycie wykonaną, zwraca zabezpieczenie.

§ 6.

1. W przypadku niezrealizowania przez Wykonawcę któregokolwiek ze szkoleń objętych umową i wynikających z voucherów, z przyczyn leżących po stronie Wykonawcy, Wykonawca zwróci Zamawiającemu wynagrodzenie za niezrealizowane szkolenie powiększone tytułem kary umownej o kwotę stanowiącą równowartość 20 % wartości niezrealizowanego zamówienia.
2. W przypadku powtarzających przez Wykonawcę naruszeń przepisów niniejszej umowy, Zamawiający po uprzednim pisemnym wezwaniu do zaniechania naruszeń ma prawo do odstąpienia od umowy. W tym przypadku Wykonawca zwróci Zamawiającemu wynagrodzenie za niezrealizowane szkolenie oraz wynagrodzenie za szkolenia mające się odbyć po dniu odstąpienia.
3. W przypadku odstąpienia od umowy przez Zamawiającego z przyczyn określonych w ust. 2, Wykonawca oprócz zwrotu wynagrodzenia, o którym mowa w ust. 2 zapłaci Zamawiającemu karę umowną w wysokości 20% wartości wszystkich niezrealizowanych szkoleń wynikających z umowy.
4. W przypadku niedostarczenia voucherów w terminie do dnia ……. (max do 16.12.2015 r.) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1000 zł za każdy dzień pozostawania w opóźnieniu.

5. W przypadku niedostarczenia voucherów w terminie do dnia ……. (max do 16.12.2015 r.) Zamawiający ma prawo odstąpić od umowy i naliczyć z tytułu odstąpienia od umowy karę umowną w wysokości 20% wynagrodzenia brutto Wykonawcy określonego w § 4 ust. 1 umowy.
6. Zamawiający ma prawo dokonywać potrąceń naliczonych kar umownych z zabezpieczenia należytego wykonania umowy lub z wynagrodzenia Wykonawcy.
7. Naliczanie kar umownych nie wyklucza dochodzenia od Wykonawcy odszkodowania na zasadach ogólnych, jeżeli wysokość kar umownych nie pokrywa wyrządzonej szkody.

§ 7.

1. Wszelkie zmiany w treści niniejszej umowy wymagają pisemnej zgody obydwu Stron w formie aneksu, pod rygorem nieważności.
2. Zamawiający przewiduje zmiany w umowie dotyczące przedmiotu zamówienia w następujących przypadkach:
   a) zmiany obowiązujących przepisów prawa,
   b) uzasadnionych przyczyn technicznych lub funkcjonalnych powodujących konieczność zmiany sposobu wykonania umowy,
   c) jeżeli zmiana jest korzystna dla Zamawiającego,
   d) w sytuacji wystąpienia problemów finansowych po stronie Zamawiającego z przyczyn od niego niezależnych. Zmiana postanowień umowy może dotyczyć m.in. zmiany zakresu przedmiotu umowy, wynagrodzenia, terminu realizacji itp. w takiej sytuacji zmianie ulegnie umowa w zakresie koniecznym do jej prawidłowej realizacji i zostanie wprowadzona aneksem,
   e) w sytuacji wystąpienia zjawisk związanych z działaniem siły wyższej (jak np. klęska żywiołowa, niepokoje społeczne, działania militarne, pożar itp.) Zmiana postanowień umowy może dotyczyć m.in. zmiany zakresu przedmiotu umowy, wynagrodzenia, terminu realizacji itp. W takiej sytuacji zmianie ulegnie umowa w zakresie koniecznym do prawidłowej realizacji i zostanie wprowadzona aneksem.
   f) zmiany osób odpowiedzialnych za realizację zamówienia, zarówno ze strony Zamawiającego, jak i Wykonawcy, zmiana danych teleadresowych, zmiany osób reprezentujących strony itp. podobne zmiany nie stanowią istotnej zmiany umowy w rozumieniu art. 144 ustawy Pzp,
3. Nie stanowi istotnej zmiany umowy w rozumieniu art. 144 ust. 1 ustawy Pzp:
   a) zmiana danych związanych z obsługą administracyjno-organizacyjną umowy (np. zmiana nr rachunku bankowego),
   b) zmiana danych teleadresowych,
   c) zmiana osób wskazanych do kontaktów między stronami.
4. Warunkiem dokonania zmian, o których mowa w pkt. 2 b), c) i e) jest złożenie wniosku przez Stronę inicjującą zmianę zawierającego:
   a) opis propozycji zmiany,
   b) uzasadnienie zmiany,
   c) obliczenie kosztów zmiany zgodnie z zasadami określonymi w Umowie, jeżeli zmiana będzie miała wpływ na wynagrodzenie Wykonawcy,
   d) opis wpływu zmiany na termin wykonania Umowy.
5. Zmiany, o których mowa w pkt. 2 b) mogą zostać dokonane, jeżeli zachodzi i jest jej uzasadnieniem co najmniej jedna z niżej wymienionych okoliczności:
   a) poprawa jakości,
   b) zmiany obowiązujących przepisów lub obowiązek dostosowania do obowiązujących przepisów.
6. Ponadto zmiany, o których mowa w pkt. 2 mogą dotyczyć:
   a) ustawowej zmiany stawki podatku VAT,

7. Zmiana umownego terminu zakończenia realizacji przedmiotu umowy możliwa jest w skutek działania siły wyższej.
8. Wyżej wskazane zmiany zostaną wprowadzone w postaci aneksu do umowy w sprawie zamówienia publicznego w przypadku zaistnienia zdarzeń wymienionych w pkt. 2. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Zamawiający może wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.
9. W razie zaistnienia 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. W takim przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.

§ 8.

1. Strony ustalają, że oprócz przypadków przewidzianych w Kodeksie Cywilnym, Zamawiającemu przysługuje prawo odstąpienia od umowy od uzyskania informacji o tym, że:
   a) nastąpi rozwiązanie przedsiębiorstwa Wykonawcy,
   b) zostanie wydany nakaz zajęcia majątku Wykonawcy,
   c) w przypadku określonym **§** 6 ust. 2,
   d) w przypadku określonym **§** 6 ust. 5,
   e) Wykonawca bez uzasadnionych przyczyn nie wykonuje przedmiotu umowy, pomimo dodatkowego wezwania Zamawiającego.
   f) wystąpi istotna zmiana okoliczności powodująca, że wykonanie umowy nie leży w interesie Zamawiającego, czego nie można było przewidzieć w chwili zawarcia umowy. Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
2. Wykonawca nie może zwolnić się od odpowiedzialności względem Zamawiającego z tego powodu, że niewykonanie lub nienależyte wykonanie umowy przez Wykonawcę było następstwem niewykonania lub nienależytego wykonania zobowiązań wobec Wykonawców przez jego Podwykonawców.
3. W przypadku odstąpienia od umowy przez Zamawiającego z przyczyn, o których mowa w ust. 1 pkt. a lub b, Wykonawca oprócz zwrotu wynagrodzenia za niezrealizowane szkolenia zapłaci Zamawiającemu karę umowną w wysokości 10 % wartości niezrealizowanych szkoleń.
4. Jeżeli skutki wystąpienia stanu „siły wyższej" trwają dłużej niż 14 dni, strony postanawiają, że po upływie tego terminu odstępują od umowy.
5. Działanie „siły wyższej" definiuje się, jako niezależne od Stron umowy zaistnienie niesprzyjającego zdarzenia losowego (pożar, powódź, katastrofa budowlana, skutki innych katastrof wiążących, zagrożenie życia ludzi, zagrożenie skażeniem środowiska, utratą mienia lub poniesieniem znacznych strat materialnych, itp.) lub szeregu takich zdarzeń, upoważniające Strony do przerwania dalszej realizacji umowy. Wystąpienie „siły wyższej" musi zostać udokumentowane poświadczeniami właściwych organów.

§ 9.

1. Strony wyznaczają swoich przedstawicieli:
   a) Zamawiający:
   ……
   b) Wykonawca:
   ……
2. Zmiana danych kontaktowych osób wymienionych powyżej nie stanowi zmiany umowy.
3. Wszelką korespondencję pomiędzy stronami wysłaną na adres wskazany w niniejszej umowie uważa się za doręczoną.

4. Ewentualne spory, wynikłe w związku z realizacją przedmiotu umowy, strony zobowiązują się rozwiązywać w drodze wspólnych negocjacji, a w przypadku niemożności ustalenia kompromisu będą rozstrzygane przez sądy powszechne wg. właściwości miejscowej Zamawiającego.
5. W sprawach, których nie reguluje niniejsza umowa, będą miały zastosowanie odpowiednie przepisy ustaw: Kodeks cywilny, Prawo budowlane i ustawa Pzp wraz z aktami wykonawczymi do tych ustaw.
6. Niniejszą umowę wraz z załącznikami sporządzono w 2 (dwóch) jednobrzmiących egzemplarzach: 1 dla Zamawiającego, 1 dla Wykonawcy.

Załącznikami do niniejszej umowy są:

Nr 1 – Opis przedmiotu umowy – formularz cenowy.

Podpis i pieczęć

WYKONAWCY ZAMAWIAJĄCEGO

Załącznik nr 10 do SIWZ

pieczęć adresowa firmy Wykonawcy

Opis przedmiotu zamówienia - formularz cenowy

Zaoferowany przez Wykonawcę program szkoleń ma być zgodny z wymaganiami.
Dla szkoleń nr:

- **1-6, 15: wymagana jest autoryzacja Red Hat.**
- **7: wymagana jest autoryzacja przez jeden z instytutów egzaminacyjnych (Examination Institute) ITIL licencjonowanych przez AXELOS - oficjalnego akredytora ITIL.**
- **18-24: wymagana jest autoryzacja szkolenia przez SANS Institute.**

ID	Nazwa	Minimalny czas trwania szkolenia (liczba dni)	Wymagana minimalna ilość osób do przeszkolenia	Szkolenie oferowane – dokładny opis oferowanego szkolenia (wymagany w przypadku oferowania szkolenia równoważnego) lub stwierdzenie „**opis szkolenia identyczny z wymaganym w SIWZ**”	Cena netto szkolenia dla wszystkich osób	Cena brutto szkolenia dla wszystkich osób
1	Red Hat System Administration I (RH319) na RHEL7	5	2			
2	Red Hat System Administration II z egzaminem RHCSA (RH135) na RHEL7	5	2			
3	Red Hat OpenStack Administration with Expertise Exam (CL211)	5	2			
4	Neutron Networking with Red Hat Enterprise Linux OpenStack Platform (CL306)	2	2			

5	High Availability with Red Hat Enterprise Linux OpenStack Platform (CL332)	2	2			
6	Red Hat Ceph Storage Architecture and Administration (CEPH 125)	5	2			
7	ITIL® Foundation	3	7			
8	Analiza Malware'u — Zaawanswany Reverse Engineering	3	4			
9	Hacking HTML5 (zaawansowane warsztaty z bezpieczeństwa webaplikacji)	2	4			
10	Szkolenie z Informatyki Śledczej (computer forensics)	2	6			
11	Bezpieczeństwo aplikacji mobilnych	2	4			
12	Szkolenie: Bezpieczeństwo Windows (praktyczne warsztaty z ochrony systemu)	3	4			
13	Szkolenie z Bezpieczeństwa Sieci Komputerowych (Testy Penetracyjne)	3	6			
14	Szkolenie z Bezpieczeństwa Webaplikacji (atakowanie i ochrona aplikacji webowych)	2	4			
15	RH 43 – Red Hat server hardening	4	2			
16	HDP02 – HDP Developer: Apache Pig and Hive	4	3			
17	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (SEC660)	5	1			
18	Mobile Device Security and Ethical Hacking (SEC575)	5	1			
19	Hacker Tools, Techniques, Exploits and Incident Handling (SEC504)	5	1			
20	Network Penetration Testing and Ethical Hacking (SEC560)	5	1			
21	Reverse-Engineering Malware: Malware Analysis Tools and Techniques (FOR610)	5	1			
22	Auditing & Monitoring Networks, Perimeters & Systems (AUD507)	5	1			

23	Advanced Network Forensics and Analysis (FOR572)	5	1			
24	Memory Forensics In-Depth (FOR526)	5	1			

Poprzez 1 dzień szkolenia należy rozumieć minimum 7, maksimum 10 godzin dydaktycznych, gdzie jedna godzina dydaktyczna wynosi minimum 45 minut.

Za równoważne, Zamawiający uzna szkolenia obejmujące, co najmniej przedmiot zawarty w szkoleniach o minimalnie takiej samej tematyce przedmiotowych szkoleń, taki samym minimalnym czasie wymagany do ich przeprowadzenia. Zamawiający wymaga również aby szkolenia równoważne posiadały odpowiednią akredytację, zgodnie z wymaganiami SIWZ (dla tych szkoleń dla których była przewidziana akredytacja).

Przy opisie zawartości szkoleń wykorzystano źródła stron internetowych firm szkoleniowych. Zamawiający nie preferuje żadnych z tych firm. Zgodnie z art. 11 pkt 1, 3–7 ustawy z dnia 7 października 1999 r. o języku polskim (Dz. U. z 1999 r. Nr 90, poz. 999) Zamawiający w opisie przedmiotu zamówienia użył terminologii angielskiej do pomocniczego określenia zakresu szkoleń - mimo że postępowanie w przedmiocie udzielenia zamówienia prowadzi się w języku polskim.

.....
(miejscowość, data)

…….....
(pieczęć imienna i podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy)

Zał. nr 11 do SIWZ

Wymagania na szkolenia dla CybrSecLab
(pomocnicze określenia zakresu szkoleń)

ID	Wymagania
1	**Red Hat System Administration I (RH124) na RHEL7** Szkolenie musi być autoryzowane przez Red Hat (na wersji Red Hat Enterprise Linux 7). Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim): *Course overview* *Red Hat System Administration I provides a foundation for students wishing to become full-time Linux system administrators by introducing key command line concepts and other enterprise-level tools. These concepts are further developed in the follow-on course, Red Hat System Administration II (RH134).* *Course content summary* *Introduction to the command line* *Managing physical storage* *Learning how to install and configure software components and services* *Establishing network connections and firewall access* *Monitoring and managing processes* *Managing and securing files* *Administrating users and groups* *Accessing Linux file systems* *Installing and using virtualized systems* *Reviewing the system log files and journal* [źródło: http://www.redhat.com]
2	**Red Hat System Administration II z egzaminem RHCSA (RH135) na RHEL7** Szkolenie musi być autoryzowane przez Red Hat (na wersji Red Hat Enterprise Linux 7). Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim): *Course overview* *Red Hat System Administration II (RH135) focuses on the key tasks needed to become a full time Linux administrator. This course goes deeper into enterprise Linux administration including file systems and partitioning, logical volumes, SELinux, firewalling, and troubleshooting. Attending both Red Hat System Administration I and Red Hat System Administration II can help you in your preparation for the Red Hat Certified System Administrator exam (EX200), which is included in this version of the*

	course. *Course content summary* *Installation using Kickstart* *Manage filesystems and logical volumes* *Manage scheduled jobs* *Access network filesystems* *Manage SELinux* *Control firewalling* *Troubleshooting* [źródło: http://www.redhat.com]
3	**Red Hat OpenStack Administration with Expertise Exam (CL211)** Szkolenie musi być autoryzowane przez Red Hat (na wersji Red Hat Enterprise Linux 7). Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim). *Course overview* *Through hands-on labs, students will explore manually installing each service of Red Hat Enterprise Linux OpenStack® Platform, and will also look at the future plans of the OpenStack development community.* *This course can also help you prepare for the Red Hat Certified System Administrator in Red Hat OpenStack exam (EX210). This version of the course includes the exam.* *Course content summary* *Get an overview of the Red Hat Enterprise Linux OpenStack Platform architecture* *Install Red Hat Enterprise Linux OpenStack Platform using packstack* *Deploy each Red Hat Enterprise Linux OpenStack Platform service manually* *Manage users and projects* *Deploy instances, and use Heat to deploy and customize instances* *Read the entire course outline for more details.* *Note: Red Hat OpenStack Administration is one of our emerging technology courses. This series of courses focuses on Red Hat's evolving technologies. Emerging technology courses are feature-and functionality-focused and are conducted like guided labs.* ***The OpenStack® Word Mark and OpenStack Logo are either registered trademarks / service marks or trademarks / service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community.***
4	**Neutron Networking with Red Hat Enterprise Linux OpenStack Platform (CL306)** Szkolenie musi być autoryzowane przez Red Hat. Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne

	szkolenie w języku polskim): *Course overview* *Overview of Neutron architecture* *Deploy Open vSwitch and Linux bridge* *Use network namespaces and virtual devices* *Install Neutron networking* *Deploy L2 services* *Deploy DHCP agents* *Deploy L3 agents* *More Details:* *Introduction to networking and OpenStack fundamentals* *Define OpenStack architecture and network protocols related to software-defined networks (SDN).* *Introduction to Linux networking fundamentals* *Review Linux system administration networking concepts.* *Deploy virtual bridges* *Install and manage Linux bridges and Open vSwitch.* *Deploy virtual network devices and implementing namespaces* *Create tap devices, veth devices, and network namespaces. Implement a virtual router.* *Introduction to Neutron architecture* *Define Neutron architecture.* *Implement and use the Neutron server* *Implement and use the Neutron L2 services* *Implement and use the Neutron DHCP agent* *Implement and use the Neutron L3 agent*
5	**High Availability with Red Hat Enterprise Linux OpenStack Platform (CL332)** Szkolenie musi być autoryzowane przez Red Hat. Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim). *Course overview* *High-availability basic concepts* *Comprehensive plan for a highly available cloud*

	Cluster a Red Hat Enterprise Linux OpenStack Platform environment using high-availability designs and implementations *Validation of the highly available cloud* *MariaDB Galera cluster for Red Hat Enterprise Linux OpenStack Platform database* *GlusterFS for Glance and Cinder* *More Details:* *Introduction to high availability* *Define how high availability can secure and improve Red Hat Enterprise Linux OpenStack Platform services.* *Deploying a high-availability cluster* *Configure Pacemaker, Corosync and HaProxy for the OpenStack API services.* *Configure Red Hat Enterprise Linux OpenStack Platform services* *Install Red Hat Enterprise Linux OpenStack Platform and configure the API services.* *Implement an active-passive MySQL cluster* *Connect the MySQL database with the highly available architecture.* *Implement an active-active Qpid broker* *Set up and run a pool of message brokers to improve availability and reliability.* *Testing the environment* *Run a unit test protocol for every service, and review and validate the high-availability services.* *Running failure scenarios* *Fail various services and test high availability.* *Implement an even more highly available cloud* *Explore innovative ways to secure your cloud data using top open source clustering solutions like MariaDB Galera and GlusterFS, a Red Hat community storage project.*
6	**Red Hat Ceph Storage Architecture and Administration (CEPH 125)** Szkolenie musi być autoryzowane przez Red Hat. Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim): *Course overview* *Introduction to course and Ceph* *Introduce the course, Ceph Storage, and related Ceph systems.* *Overview of Ceph components* *Provide an overview of the requirements to create and access object storage data in Ceph Object Store.* *Overview of CRUSH map*

	Understand CRUSH data placement algorithm and how it is used to determine data placement. *Ceph Block storage* *Describe the method to create and access block storage data with the Ceph Block device (RBD).* *Ceph Filesystem* *Describe the method to create and access file storage data with the Ceph distributed file system.* *Ceph Storage cluster* *Create a Ceph object cluster.* *Ceph file* *Configure a Ceph file in Global, MON, MDS, and OSD server sections.* *Ceph clients* *Work with Ceph object clusters, Ceph Block Devices, Ceph Object Gateway daemons, and Ceph Filesystem.* *Ceph pools* *Understand Ceph pool concepts and configuration.* *CRUSH map configuration* *Configure and manage CRUSH map.* *MON servers* *Explain and create MON servers.* *OSD servers* *Explain and create Ceph OSD servers and OSD Maps.* *MDS servers* *Overview, configure, and map MDS servers.* *Alternative deployment* *Overview alternative deployment methods.* *Ceph operations & maintenance* *Overview and troubleshoot daily maintenance with Ceph.* *Performance tuning* *Tune the Linux server.* *Ceph daemon optimization* *Overview and optimize Ceph daemons.* *Architectural considerations* *Discuss architectural considerations for Ceph Performance Optimization.* *Ceph Client tuning & troubleshooting* *Tune and troubleshoot Ceph Client.*

	Introduction to OpenStack & Ceph *Introduce and explain integration of Ceph and OpenStack.* *Integrate Ceph with Glance* *Integrate object storage for image with Glance.* *Integrate Ceph with Cinder* *Integrate block storage for VMs with Cinder.* *Ceph and Ceph Object Gateway daemons* *Overview process to replace Swift with Ceph and Ceph Object Gateway daemons.*
7	**Szkolenie ITIL® Foundation z egzaminem ITIL® Foundation** Szkolenie akredytowane, realizowane przy współpracy z Akredytowaną Organizacją Szkoleniową. Program zgodny z zaleceniami akredytacji. Szkolenie obejmuje także egzamin pozwalający uzyskać certyfikat ITIL® Foundation.
8	**Analiza Malware'u — Zaawanswany Reverse Engineering** Dedykowane szkolenie specjalistyczne. Wymagany zakres szkolenia: *1. Wprowadzenie do świata malware'u* *2. Budowanie podejścia* *ustalenie typu malware'u* *ustalenie najważniejszych elementów analizy* *narzędzia* *jak pozyskiwać próbki do analizy* *Omówienie różnych technik i metodyki analizy na podstawie odmiennych typów malawre'u* *3. Trojan-Dropper* *badanie zasobów oraz "monitorowanie miejsca zrzutu"* *analiza algorytmów szyfrowania i ich zastosowania* *badanie entropii* *tworzenie deszyfratora* *techniki uzyskiwania odszyfrowanych danych bez potrzeby tworzenia deszyfratora* *wstęp do BHO* *4. Banker pisany w Delphi (Infostealer.Bancos)* *określenie targetu na podstawie zawartości zasobów* *zapoznanie z narzędziami ułatwiającymi analizę malwareu pisanego w Delphi* *— pliki MAP* *— sygnatury*

	analiza prostej techniki monitorowania odwiedzanych stron przez użytkownika *przechwytywanie skradzionych danych* *— kontrolowanie przepływu danych* *5.Wykorzystanie gotowego kodu* *sterowanie wykonaniem instrukcji (ImmunityDebugger + immlib)* *traktowanie binarnego pliku, jako funkcji* *6. KeyLoggers* *rozpoznanie technik powiązanych z keyloggerami* *analiza technik* *7. Banker pisany w VisualBasicu* *zapoznanie z narzędziami ułatwiającymi analizę malwareu pisanego w VB* *omówienie najistotniejszych cech reversowanego kodu VB* *8. Analiza techniki wykorzystywanych do monitorowania oraz modyfikacji odwiedzanych stron (HTML injection)* *monitorowanie aktywności InternetExplorera* *— BHO* *— interface IWebBrowser* *pozostałe przeglądarki* *— inline hooking* *9. Dll injection* *analiza metod* *10. Analiza sposobów na podpięcie się pod proces dziecko.* *JIT & 0xCC* *0xEBFE* *Global Flags* *11. Wykrywanie wirtualnej maszyny* *analiza technik* *jak to robił Sinowal (Torpig)* *12. Analiza rootkitów* *analiza instalacji rootkita w systemie* *omówienie api wykorzystywanych przez rootkity.* *IDT hooking* *ochrona komponentów malware'u* *SSDT hooking*

9	**Hacking HTML5 (zaawansowane warsztaty z bezpieczeństwa webaplikacji)** Dedykowane szkolenie specjalistyczne. Wymagany zakres szkolenia: *HTML 5 – wstęp* *Same origin policy – założenia i szczegóły techniczne* *XSS* *— nowe wektory ataków w HTML5* *— ataki przy zablokowanym JavaScript* *— nowe możliwości ukrywania ataków* *— omijanie zabezpieczeń filtrów* *Cross document messaging* *— możliwości technologii* *— ataki i obrona* *Cross Origin Resource Sharing* *— zmiany w same origin policy i konsekwencie* *— przykład włamania do aplikacji HTML4 dzięki HTML5* *— jak zabezpieczyć aplikację* *Offline Web Applications, przechowywanie danych po stronie klienta* *— możliwości* *— implementacja* *— wykorzystanie w atakach (sidejacking i cache poisoning)* *— evercookie* *Web SQL* *— możliwości* *— atakowanie i zabezpieczanie* *Web Sockets* *— możliwości* *— architektura* *— tworzenie i atakowanie aplikacji opartych o WebSockets* *— jak poprawnie implementować serwer WebSockets* *Web Workers* *— możliwości API*

	— bezpieczne użycie Web Workers *— ataki z użyciem Web Workers* *Filtry Anti-XSS w przelgądarkach* *— zasada działania* *— skuteczne omijanie filtrów* *IFrame w HTML5* *— nowe funkcjonalności i sandboxing* *— nowe podatności* *— next generation clickjacking* *— nowe możliwości ataków clickjacking, również na aplikacje HTML4* *— jak zabezpieczyć aplikację* *Geolokalizacja* *— zasada działania geolokalizacji* *Canvas – omówienie kwestii bezpieczeństwa* *Atakowanie przy użyciu SVG* *Ataki E4X* *Narzędzia do przeprowadzania ataków HTML5* *Podsumowanie*
10	**Szkolenie z Informatyki Śledczej (computer forensics)** Dedykowane szkolenie specjalistyczne z ćwiczeniami, które wynosić będą min. 70% czasu całego szkolenia. Wymagany minimalny zakres szkolenia: *DOWÓD ELEKTRONICZNY* *– pojęcie dowodu elektronicznego* *– najlepsze praktyki informatyki śledczej* *– procedury i polityki w firmach* *– aspekty prawne* *– rola i zadania Forensics Analyst, Investigator, Examiner* *PROCESY I PROCEDURY W INFORMATYCE ŚLEDCZEJ* ** identyfikacja:* *– planowanie i rozpoznanie możliwości dowodowych* *– oględziny miejsca zdarzenia,* *– identyfikacja sprzętu, urządzeń przenośnych, urządzeń mobilnych, analogowych dokumentów* *– dokumentowanie miejsca zdarzenia*

	– łańcuch dowodowy *LAB: oględziny miejsca zdarzenia* ** zabezpieczenie:* *– ulotność danych* *– zabezpieczenie „live" vs. post mortem* *– klonowanie dysków (metody hardwareowe i softwareowe)* *– sterylność dysków docelowych* *– formaty obrazów* *– funkcje skrótu (MD5, SHA256)LAB: permanentne czyszczenie dysku, wykonywanie kopii binarnej dysku* ** analiza:* *– rodzaje informacji przechowywanych na cyfrowych nośnikach informacji* *– odzyskiwanie danych* *– przeszukiwanie przestrzeni przydzielonej, nieprzydzielonej, slack space* *– dokumentowanie przeprowadzonych badań* *– korelacja artefaktów* *LAB: rekonstrukcja przebiegu przykładowego nadużycia* ** raportowanie:* *– konstrukcja raportu* *– raportowanie metodą KISS* *– prezentacja dla Zarządu* *LAB: ocena merytoryczna przykładowych raportów* *OPROGRAMOWANIE (KOMERCYJNE I OPEN-SOURCE)* *– funkcjonalność komercyjnych programów: np. FTK oraz X-Ways Forensic* *– narzędzia do badania telefonów komórkowych (np. UFED, Oxygen Analyst)* *– funkcjonalności narzędzi open source (np. CAINE, DEFT, NirSoft, RegRipper)* *ANALIZA ŚLEDCZA SYSTEMU OPERACYJNEGO WINDOWS* *– analiza artefaktów Windows* *– analiza logów systemowych* *– analiza wybranych elementów rejestrów systemowych* *– analiza skompresowanych plików* *– pliki i katalogi użytkownika*

	– analiza zawartości kosza systemowego *– analiza Thumbs.db oraz plików .lnk* *ANALIZA ŚLEDCZA PRZEGLĄDAREK INTERNETOWYCH, KOMUNIKATORÓW I SŁÓW KLUCZOWYCH* *– artefakty najczęściej spotykanych przeglądarek (minimum Internet Explorer, Mozilla Firefox, Google Chrome)* *– pliki historii internetowych, ciasteczka (cookies), pamięć podręczna i jej zawartość (cache)* *– przegląd najpopularniejszych komunikatorów (minimum GG, Skype)* *– zaawansowane techniki przeszukiwania nośników: strings, słowa kluczowe, grep* *PRAKTYCZNA ANALIZA ŚLEDCZA PRZYGOTOWANYCH MATERIAŁÓW DOWODOWYCH*
11	**Bezpieczeństwo aplikacji mobilnych** Dedykowane szkolenie specjalistyczne. Proponowany zakres szkolenia: *1. Architektury mobilnych systemów operacyjnych (minimum iOS, Android, Windows Phone 8)* *2. Bezpieczeństwo z perspektywy użytkownika urządzenia:* *• domyślnie dostępne sposoby zabezpieczeń urządzeń w danych systemach* *• wpływ domyślnych zabezpieczeń urządzeń na bezpieczeństwo aplikacji* *• data wiping* *3. Mechanizmy bezpieczeństwa dostarczane developerom przez producentów systemów. Między innymi:* *• system uprawnień (Android)* *• Data Protection (iOS)* *• Keychain (iOS)* *4. Przełamywanie zabezpieczeń systemów:* *• eskalacja uprawnień w systemach mobilnych (jailbreak)* *• wpływ eskalacji uprawnień na bezpieczeństwo aplikacji* *• dostęp do danych użytkowników (m.in. SMS, e-mail, dane GPS)* *• analiza systemu plików (ich struktur i typów)* *• przełamywanie szyfrowania danych* *5. Bezpieczeństwo danych:* *• zagrożenia związane z wykradaniem danych na przykładzie prawdziwych zdarzeń* *• sposoby bezpiecznego przechowywanie kluczowych danych (login, hasło, klucze, dane osobowe)* *• implementowanie szyfrowania w aplikacjach mobilnych* *• zabezpieczanie aplikacji hasłem dostępowym* *• bezpieczna komunikacja pomiędzy aplikacjami (wymiana danych) oraz komponentami (Android: Activity, Service, Broadcast receiver, Content Resolver)* *• szyfrowanie baz danych*

	6. Bezpieczeństwo komunikacji: *• zagrożenia płynące z "transportu" danych* *• poprawna, bezpieczna implementacja aplikacji klient-serwer* *• mechanizmy szyfrowania (minimum SSL/TLS)* *• wykorzystanie PKI (Public Key Infrastructure)* *7. Bezpieczeństwo aplikacji:* *• analiza sposobów dystrybucji aplikacji i ryzyka z nią związane* *• analiza form binarnych aplikacji i ich dystrybucji (minimum odex, Mach-O, ipa, apk)* *• Reverse Engineering aplikacji (minimum Cycript, baksmali, apktool)* *• utrudnianie analizy kodu i modyfikacji działania aplikacji (m.in. blokowanie debugerów, obfuskacja kodu, ASLR)* *• wykrywanie środowisk z podwyższonymi uprawnieniami (jailbreak)* *• narzędzia wspomagające analizę bezpieczeństwa aplikacji* *8. Istotne mechanizmy specyficzne dla platform i ataki z nimi związane. Między innymi:* *• multitasking (app state/GUI caching)* *• wprowadzanie danych (input caching)* *• zanużanie aplikacji webowych (CSRF, framing, clickjacking)* *• identyfikacja urządzeń i użytkowników (UDID)* *• push notifications* *• tapjacking* *• zarządzanie logami* *9. Ciekawe przypadki przełamywania zabezpieczeń – case studies.* *10. Omówienie implikacji stosowania zaleceń NIST: Guidelines for Managing the Security of Mobile Devices in the Enterprise, a także Google Android Benchmarks oraz Apple iOS Benchmarks.*
12	**Szkolenie: Bezpieczeństwo Windows (praktyczne warsztaty z ochrony systemu)** Dedykowane szkolenie specjalistyczne. Wymagany zakres szkolenia: *Centralne zarządzanie konfiguracją:* ○ *Access Control List – ograniczenie dla zwykłego użytkownika do tworzenia plików tylko i wyłącznie w profilu,* ○ *Auditing – ustawienia audytu zdarzeń w systemie,* ○ *Eventlog – ustawienia, archiwizacja logów,* ○ *Event Forwarding – centralna archiwizacja logów,* ○ *User Rights – uprawnienia użytkownika w systemie,* ○ *Restricted Groups – zarządzanie przynależnością do grup lokalnych,*

	○ *Security Options – opcje bezpieczeństwa systemu,* ○ *Services – usługi systemowe,* ○ *AppLocker – ograniczenie uruchamianych aplikacji tylko do autoryzowanych,* ○ *IPSec – uzupełnienie np. Cisco ISE, wzajemna autoryzacja urządzeń,* ○ *Windows Firewall – systemowa zapora sieciowa,* ○ *Preferences – specyficzne zmiany w rejestrach, np. konfiguracja Adobe Reader, Java,* *Bezpieczne środowisko pracy:* ○ *Internet Explorer 11,* ○ *Office 2013,* ○ *Adobe Reader,* ○ *Adobe Flash,* ○ *Java.* *EMET 5.1 – ograniczenie podatności na ataki,* *Microsoft Message Analyzer 1.2 jako analizator sieciowy,* *Sysinternal Suite – pakiet przydatnych narzędzi np. AccessChk, Procmon.* *Microsoft Security Compliance Manager – zbiór ustawień dla Microsoft,* *DeviceLock – zarządzanie między innymi USB,* *Folder Redirection – odmiejscowienie danych użytkownika (bezpieczeństwo danych),* *Integrity Levels,* *Internet Explorer Enterprise Mode,* *RMS – (w porównaniu do DLP),* *Security Essential jako AV (w miarę dostępnego czasu),* *BONUS: IBM Security Trusteer Rapport jako przykład ochrony stron internetowych (client-side*
13	**Szkolenie z Bezpieczeństwa Sieci Komputerowych (Testy Penetracyjne)** Dedykowane szkolenie specjalistyczne z ćwiczeniami (ćwiczenia mają trwać nie krócej niż 70% czasu szkolenia). Wymagany zakres szkolenia: *1. Wprowadzenie do testów penetracyjnych* *metodyki i rodzaje pentestów* *OSSTMM / OWASP* *Dokumenty opisujące dobre praktyki (NIST/CIS)* *różnice pomiędzy pentestami a audytami* *2. Organizacja testów penetracyjnych*

	prawne aspekty prowadzenia testów penetracyjnch *opracowanie planu testów penetracyjnych* *popularne problemy spotykane podczas testów penetracyjnych* *3. Poszczególne fazy testu penetracyjnego* *» Rekonesans* *pasywne metody zbierania informacji o celu* *wykorzystanie serwerów proxy* *zbieranie i analiza metadanych* *social-engineering, profilowanie pracowników i APT* *aktywne metody zbierania informacji o celu* *mapowanie sieci ofiary* *omijanie firewalli* *» Enumeracja podatności* *rodzaje podatności (buffer overflow, format string, etc.)* *shellcode?* *mechanizmy DEP/ASLR i ich omijanie* *ROP i heap spray'ing* *dopasowywanie kodu exploita do znalezionych podatności* *rodzaje exploitów* *wyszukiwanie exploitów* *analiza przykładowego exploita* *tworzenie własnego exploita* *wybór drogi wejścia do systemu* *» Atak* *przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe* *ataki w sieci LAN/WAN/Wi-Fi* *ataki na urządzenia sieciowe (routery, switche, IDS/IPS/WAF, firewalle, load balancery)* *ataki denial of service* *fuzzing* *łamanie haseł* *atak przy pomocy exploita zdalnego* *narzędzia wspomagające atak* *podniesienie uprawnień do poziomu administratora*

	exploity lokalne *łamanie hashy haseł* *» Zacieranie śladów* *Backdoor, rootkit* *backdoorowanie przejętego systemu* *zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej* *» Sporządzenie raportu z testu penetracyjnego* *budowa szczegółowego raportu technicznego* *raport dla zarządu* *4. Metody ochrony przed atakami* *idea honeypotów* *systemy IDS/IPS* *metody hardeningu systemów Windows* *metody hardeningu systemów Linux*
14	**Szkolenie z Bezpieczeństwa Webaplikacji (atakowanie i ochrona aplikacji webowych**) Dedykowane szkolenie specjalistyczne. Proponowany zakres szkolenia: Współczesne problemy bezpieczeństwa aplikacji webowych *zagrożenia wynikające z architektury webaplikacji (np. CGI, SSI, etc.)* *zagrożenia wynikające z języków programowania (PHP, ASP, JSP, JS, etc.)* *problem styku webaplikacji z bazą danych* *interfejsy zewnętrzne webaplikacji* *zagrożenia po stronie serwera, środowiska, sieci, a zagrożenia po stronie klienta* *zagrożenia stron tworzonych pod urządzenia mobilne (telefony, tablety)* *Ataki na aplikacje webowe* *Wyszukiwanie adresów serwerów deweloperskich* *Bezpieczeństwo hostingu i webserwera* *Brak obsługi błędów* *Manipulacje parametrami (metody GET, POST)* *Techniki podsłuchu i manipulowania transmisją* *Atak Forcefull browsing* *Atak Path Traversal*

	Technika Google Hacking *Wstrzyknięcie kodu (PHP shell) i komend systemowych do webaplikacji* *Problem filtrowania danych wejściowych* *Ataki XSS (persistent, reflected)* *Omijanie filtrowania danych wejściowych i encodingu wyjściowych* *Ataki na sesję aplikacji webowej* *Podsłuchiwanie sesji i kradzież ciasteczek HTTP* *Ataki Session Fixation i Session Adoption* *Jak poprawnie zarządzać sesją w webapikacji?* *Ataki CSRF* *Ataki Tabnabbing oraz Clickjacking* *Ataki na bazy danych* *Ataki SQL injection i Blind SQL injection* *Cechy charakterystyczne środowisk Oracle, Microsoft SQL, MySQL i PostgreSQL* *Ochrona przed atakami SQL injection* *Szyfrowanie połączenia i ataki na SSL* *Szyfrowanie danych w webaplikacji* *Ochrona przed spamem i enumeracją zasobów oraz haseł* *Podsumowanie zagrożeń i przegląd OWASP TOP10* *Pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF)* *Omijanie detekcji przez systemy WAF/IDS/IPS* *Problemy przeglądarek* *Same Orgin Policy* *Rich Internet Applications* *Dziury w przeglądarkach* *Ataki DNS-Rebinding* *Wtyczki i rozszerzenia podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych*
15	RH 413 – Red Hat server hardening Szkolenie musi być autoryzowane przez Red Hat. Program szkolenia musi być zgodny z tematyką określaną przez Red Hat. Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim). *Course content summary* *Review errata and apply them to Red Hat Enterprise Linux*

	Use special permissions and file system access control lists *Manage users and password-aging policy requirements* *Install and configure Red Hat Identity Management tools* *Understand system auditing*
16	**HDP02 – HDP Developer: Apache Pig and Hive** Dedykowane szkolenie specjalistyczne z ćwiczeniami (min 70% szkolenia). Wymagany zakres szkolenia w języku angielskim (Wykonawca może zaoferować równoznaczne szkolenie w języku polskim): Understanding Hadoop 2.0 The Hadoop Distributed File System (HDFS) Inputting Data into HDFS The MapReduce Framework and YARN Introduction to Pig Advanced Pig Programming Hive Programming Using HCatalog Advanced Hive Programming Advanced Hive Programming (cont.) Data Analysis and Statistics Defining Workflow with Oozie Practical exercises: Use HDFS commands to add/remove files and folders from HDFS Use Sqoop to transfer data between HDFS and a RDBMS Run a MapReduce job Run a YARN application Explore and transform data using Pig Split a dataset using Pig Join two datasets using Pig Use Pig to transform and export a dataset for use with Hive Use HCatLoader and HCatStorer to retrieve HCatalog schemas from within a Pig script Understand how a Hive table is stored in HDFS Use Hive to discover useful information in a dataset Understand how Hive queries get executed as MapReduce jobs Perform a join of two datasets with Hive

	Use advanced Hive features like windowing, views and ORC files Use the Hive analytics functions (rank, dense_rank, cume_dist, row_number) Write a custom reducer in Python that reduces the number of underlying MapReduce jobs generated from a Hive query Analyze and sessionize clickstream data using the Pig DataFu library Compute quantiles of NYSE stock prices Use Hive to compute ngrams on Avro-formatted files
17	**Advanced Penetration Testing, Exploit Writing, and Ethical Hacking (SEC660)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. *SEC660.1: Network Attacks for Penetration Testers* *SEC660.2: Crypto, Network Booting Attacks, and Escaping Restricted Environments* *SEC660.3: Python, Scapy, and Fuzzing* *SEC660.4: Exploiting Linux for Penetration Testers* *SEC660.5: Exploiting Windows for Penetration Testers* *SEC660.6: Capture the Flag*
18	**Mobile Device Security and Ethical Hacking (SEC575)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *SEC575.1: Device Architecture and Common Mobile Threats* *SEC575.2: Mobile Platform Access and Application Analysis* *SEC575.3: Mobile Application Reverse Engineering* *SEC575.4: Penetration Testing Mobile Devices, Part 1* *SEC575.5: Penetration Testing Mobile Devices, Part 2* *SEC575.6: Capture the Flag*
19	**Hacker Tools, Techniques, Exploits and Incident Handling (SEC504)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute.

	Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *SEC504.1: Incident Handling Step-by-Step and Computer Crime Investigation* *SEC504.2: Computer and Network Hacker Exploits - Part 1* *SEC504.3: Computer and Network Hacker Exploits - Part 2* *SEC504.4: Computer and Network Hacker Exploits - Part 3* *SEC504.5: Computer and Network Hacker Exploits - Part 4* *SEC504.6: Hacker Tools Workshop*
20	**Network Penetration Testing and Ethical Hacking (SEC560)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *SEC560.1: Comprehensive Pen Test Planning, Scoping and Recon* *SEC560.2: In-Depth Scanning* *SEC560.3: Exploitation and Post-Exploitation* *SEC560.4: Password Attacks and Merciless Pivoting* *SEC560.5: Wireless and Web Apps Penetration Testing* *SEC560.6: Penetration Testing Workshop and Capture the Flag Event*
21	**Reverse-Engineering Malware: Malware Analysis Tools and Techniques (FOR610)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *FOR610.1: Malware Analysis Fundamentals* *FOR610.2: Malicious Code Analysis* *FOR610.3: In-Depth Malware Analysis* *FOR610.4: Self-Defending Malware* *FOR610.5: Malicious Documents and Memory Forensics* *FOR610.6: Malware Analysis Tournament*

22	**Auditing & Monitoring Networks, Perimeters & Systems (AUD507**) Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *AUD507.1: Effective Auditing, Risk Assessment, Reporting* *AUD507.2: Effective Network & Perimeter Auditing / Monitoring* *AUD507.3: Web Application Auditing* *AUD507.4: Advanced Windows Auditing & Monitoring* *AUD507.5: Advanced Unix Auditing & Monitoring* *AUD507.6: Audit the Flag: A NetWars Experience*
23	**Advanced Network Forensics and Analysis (FOR572)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *FOR572.1: Off the Disk and Onto the Wire* *FOR572.2: NetFlow Analysis, Commerical Tools, and Visualization* *FOR572.3: Network Protocols and Wireless Investigations* *FOR572.4: Logging, OPSEC, allenge*
24	**Memory Forensics In-Depth (FOR526)** Szkolenie musi być autoryzowane przez SANS Institute. Program zgodny z tematyką określaną przez SANS Institute. Wymagany zakres szkolenia w języku angielskim. Wykonawca może zaoferować równoważne szkolenie w języku polskim. Szkolenie to niezależnie od wersji językowej musi być autoryzowane przez SANS Institute. Zakres szkolenia: *FOR526.1: Foundations in Memory Analysis and Acquisition* *FOR526.2: Unstructured Analysis and Process Exploration* *FOR526.3: Investigating the User via Memory Artifacts* *FOR526.4: Internal Memory Structures* *FOR526.5: Memory Analysis on Platforms Other than Windows*

	FOR526.6: Memory Analysis Challenges

Wszystkie powyższe szkolenia mają odbywać się w trybie stacjonarnym. Szkolenia muszą odbywać się w języku polskim lub angielskim.
Zaoferowany przez Wykonawcę program szkoleń ma być zgodny z wymaganiami.
Dla szkoleń nr:

- **1-6, 15: wymagana jest autoryzacja Red Hat.**
- **7: wymagana jest autoryzacja przez jeden z instytutów egzaminacyjnych (Examination Institute) ITIL licencjonowanych przez AXELOS - oficjalnego akredytora ITIL.**
- **18-24: wymagana jest autoryzacja szkolenia przez SANS Institute.**

Przy opisie zawartości szkoleń wykorzystano źródła stron internetowych firm szkoleniowych. Zamawiający nie preferuje żadnych z tych firm.
Zgodnie z art. 11 pkt 1, 3–7 ustawy z dnia 7 października 1999 r. o języku polskim (Dz.U. z 1999 r. Nr 90, poz. 999) Zamawiający w opisie przedmiotu zamówienia użył terminologii angielskiej do pomocniczego określenia zakresu szkoleń - mimo że postępowanie w przedmiocie udzielenia zamówienia prowadzi się w języku polskim.