Załącznik nr 1 do SIWZ

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest zakup systemu publikacji usług do Internetu. System powinien zastąpić obecnie pracujący system Microsoft Threat Management Gateway 2010 (TMG 2010).

W szczególności przedmiot zamówienia obejmuje następujące zadania do realizacji przez Wykonawcę:

1. Dostawa oraz wdrożenie wyspecyfikowanego sprzętu wraz ze standardową, dołączaną przez producenta danego urządzenia dokumentacją, oraz dostawa dodatkowych elementów infrastruktury, jeśli będą niezbędne do prawidłowego wdrożenia.
2. Dostawa oraz wdrożenie wyspecyfikowanego oprogramowania.
3. Przeniesienie usług obecnie pracujących na systemie TMG na nowy system.
4. Realizacja szkolenia.

Przed wdrożeniem Wykonawca zobowiązany jest do przygotowanie projektu technicznego dla systemu w uzgodnieniu z Zamawiającym a po wdrożeniu wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację rozwiązania.

Wykonawca udzieli Zamawiającemu minimum 36-miesięcznej gwarancji na cały dostarczony system (urządzenia, oprogramowanie). Czas gwarancji będzie liczony od daty podpisania protokołu odbioru wdrożonego systemu. Gwarancja obejmuje zobowiązanie Wykonawcy do terminowego usuwania wad i usterek.

Wykonawca zapewni świadczenie płatnej asysty technicznej w łącznej liczbie 300 godzin.

I. Uwarunkowania dla zadania oraz opis posiadanego przez Zamawiającego środowiska

Prace wdrożeniowe i konfiguracyjne będą realizowane w Podstawowym Centrum Przetwarzania Danych GUS w Warszawie – al. Niepodległości 208.
Z uwagi na fakt, iż prace wdrożeniowe i rekonfiguracyjne będą prowadzone na działającym środowisku sprzętowo–systemowo–aplikacyjnym, wymagane jest zachowanie ciągłości działania tego środowiska oraz minimalizacja przestojów. Możliwe też będzie wymaganie przeprowadzenie niektórych prac poza godzinami pracy GUS oraz innych jednostek statystyki publicznej.
Zamawiający posiada środowisko serwerowe z zainstalowanymi systemami operacyjnym MS Windows Server 2008 R2, Windows Server 2012 oraz systemami Linux a także środowisko do wirtualizacji serwerów bazujących na oprogramowaniu VMware vCenter 5.1. W środowisku pracuje system usług katalogowych bazujący na Microsoft Active Directory w wersji Windows 2008 R2 oraz system poczty Microsoft Exchange 2010.

Obecny system jest elementem systemu bezpieczeństwa sieci statystyki publicznej. Wypracowany został model udostępniania do Internetu usług WWW i innych serwisów dostępnych z poziomu Internetu. Metoda ta oparta o wykorzystanie funkcjonalności reverse-proxy systemu Threat Management Gateway 2010 (TMG) i jego mechanizmu bezpieczeństwa, skutkuje znacznym podniesieniem zabezpieczeń prezentowanych do Internetu usług, poprzez „maskowanie" rzeczywistego serwera, oferującego daną usługę, serwerami systemu TMG. Mechanizm udostępniania usług przez system TMG jest bardzo wydajny i od lat sprawdza się w systemie

statystyki. Jednak ze względu na kończące się wsparcie producenta na system TMG należy zastąpić go nowym system posiadający podobne funkcjonalności.

Obecny system TMG jest posadowiony na platformie Windows 2008 R2 i pełni następujące funkcje:

- Udostępnianie usługi forward Proxy (WebProxy)
- Udostępnianie publikacji usług WWW
- Udostępnianie publikacji pozostałych usług (np. pocztowych)
- Udostępnianie usługi VPN

TMG posiada bardzo duży zakres możliwości. Jest między innymi filtrem ruchu sieciowego, ponieważ przepuszcza tylko ruch uprawniony. Filtry warstwy aplikacji wychwytują anomalie w ramach danego protokołu TCP. Analizator ruchu wychwytuje podejrzane zachowanie hostów. W warstwie usług WebProxy system, w imieniu klientów usługi, łączy się z hostami w Internecie. TMG pełni kluczową rolę w udostępnianiu usług WEB poczty korporacyjnej (MS-Exchange 2010) na zewnątrz (Outlook WebApp, Outlook Anywhere, Active Sync), zapewniając ich bezpieczną publikację oraz odpowiednią autoryzację użytkowników. Uwierzytelnianie użytkownika i autoryzacja dostępu do usług poczty MS-Exchange oparta jest o usługę katalogową Active Directory. TMG publikuje również usługi SMTP umożliwiając chronioną wysyłkę/odbieranie poczty do/z Internetu. System TMG składa się z 7 serwerów:

- 3 serwerów z rolą FireWall – udostępniających funkcje TMG
- 2 serwerów przechowujących konfigurację TMG
- 2 serwerów udostępniających usługę Pulpit zdalny dla klientów VPN

TMG prowadzi własny segment sieci tzw. DMZ, w którym posadowione są serwery hostujące usługi, następnie publikowane do Internetu za pomocą TMG. W segmencie tym znajduje się obecnie ponad 50 serwerów (głównie wirtualnych), dla których serwisy hostuje TMG.
System udostępnia usługę VPN (Virtual Private Network) umożliwiającą dostęp z Internetu do określonych zasobów dzięki strukturze logicznej wydzielonej sieci. Uwierzytelnianie użytkownika i autoryzacja dostępu do VPN oparta jest o usługę katalogową Active Directory.

Szczegółowy opis środowiska Zamawiającego

- Zamawiający posiada domenę produkcyjną AD DS. (Microsoft Active Directory) Windows Serwer 2012 R2 o funkcjonalności lasu i domeny na poziomie Windows Server 2008 R2.
- Środowisko Statystyki Publicznej jest rozproszone. Składa się z lokalizacji centralnej, 17 lokalizacji głównych oraz 50 oddziałów i jednostek terenowych, spiętych siecią WAN.
- Sieć teleinformatyczna Statystyki Publicznej ma jeden punkt styku z Internetem umiejscowiony w lokalizacji centralnej.
- Stacje robocze użytkowników (komputery stacjonarne, przenośne i wirtualne PC) są członkami domeny i pracują pod kontrolą systemu operacyjnego Microsoft Windows w wersji 10 oraz Windows 7.
- Podstawowym oprogramowaniem biurowym użytkowanym na stacjach roboczych jest Microsoft Office w wersji co najmniej 2007.
- Poczta korporacyjna Statystyki Publicznej działa w oparciu o Microsoft Exchange Server 2010 SP3 RU18. System pocztowy jest scentralizowany – wszystkie serwery pocztowe znajdują się w lokalizacji centralnej.
- Środowisko Statystyki Publicznej posiada instalacje Microsoft SharePoint w wersji 2013.

- Infrastruktura informatyczna Statystyki publicznej objęta jest monitorowaniem za pomocą oprogramowania Microsoft SCOM (System Center Operations Manager) 2012 R2
- Statystyka publiczna posiada urządzenie brzegowe (firewall): CheckPoint R80.10,
- Statystyka publiczna posiada wdrożony system PKI (Centrum Certyfikacji) na bazie Microsoft Windows Server 2012 R2. System PKI jest zbudowany w modelu dwuwarstwowym: Offline Root CA i Active Directory Integrated CA.

Statystyka publiczna posiada wdrożony system zarządzania stacjami roboczymi i serwerami Microsoft System Center Configuration Manager 2012 R2.

II. Szczegółowa specyfikacja i opisy zadań do realizacji przez Wykonawcę.

Zadanie 1. Dostawa i wdrożenie wyspecyfikowanego sprzętu

Zamawiający wymaga dostarczenia sprzętu:

- fabrycznie nowego, nie używane wcześniej w innych projektach (nie dopuszcza się rozwiązań typu „refubrished" itp.)
- objętego opieką gwarancyjną
- posiadającego najnowszą dostępną w dniu składania ofert wersję oprogramowania

Do systemu udostępniana usługi VPN oraz publikacji usług WWW i pozostałych wskazanych przez Zamawiającego wymagane jest dostarczenie:

1) **minimum dwóch fizycznych urządzeń tego samego typu pracujących w klastrze o wysokiej dostępności** (HA) w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1. Każde urządzenie z minimum dwoma zasilaczami, umożliwiającymi ciągłą prace po uszkodzeniu zasilacza lub jednego łącza zasilającego. Pojedyncze urządzenie sieciowe musi spełniać wymogi przedstawione w tabeli 1 oraz opisane poniżej tabeli wymogi funkcjonalne.
2) **UPS** rackowy do zaproponowanych urządzeń, który musi spełniać wymogi przedstawione w tabeli 2.

Tabela 1 Urządzenie do publikacji usług i udostępniania VPN

Lp.	Parametr	Wymagania minimalne
1.	Pamięć RAM	16 GB
2.	Interfejsy seciowe	6x10/100/1000 Base-T oraz 2 x 10GE SFP+
3.	Ilość zasilaczy	2
4.	Przepływność dla warstwy 7 (L7 throughput)	5 Gbps z możliwością rozszerzenia na tym samym urządzeniu do 10 Gbps (np. przez rozszerzenie licencji)
5.	Wydajność HTTP Request na sekundę w warstwie L7	700 000 z możliwością rozszerzenia do 900 000 w tym

		samym urządzeniu (np. przez rozszerzenie licencji)
6.	Wydajność SSL transakcje/sek dla długości klucza 2048	6 000 z możliwością rozszerzenia do 12 000 w tym samym urządzeniu (np. przez rozszerzenie licencji)
7.	ECDHE transakcje/sek	Minimum 1 700 z możliwością rozszerzenia do 6 000 w tym samym urządzeniu (np. przez rozszerzenie licencji)
8.	Przepływność SSL (throughput)	5 Gbps z możliwością rozszerzenia do 10 Gbps w tym samym urządzeniu (np. przez rozszerzenie licencji)
9.	Obudowa	Przeznaczona do montażu w szafie rack 19", wysokość nie większa niż 2U
10.	Zasilanie	Redundantne 230V AC (każde urządzenie wchodzące w skład systemu)

System musi zapewniać bezpieczny i niezawodny dostęp do aplikacji web oraz spełniać poniższe wymagania.

1. Funkcjonalności dostępne dla każdego z urządzeń

    - Równoważenie obciążenia (Load balancing) w warstwie 4
    - Przełączanie według zawartości (Content switching) w warstwie
    - Obsługa protokołu IPv6
    - Carrier-Grade Network Address Translation (CGNAT)
    - Możliwość segmentacji ruchu sieciowego dla różnych aplikacji
    - Obsługiwane protokoły dynamicznego rutingu – RIP v2, OSFP, BGP, RIPng for IPv6, OSFP v3 for IPv6, IS-IS
    - Automatyczna optymalizacja protokołu TCP
2. Ochrona aplikacji

    - Ochrona przed DoS w warstwie 4 i 7
    - Wielopoziomowe uwierzytelnianie
    - Administracja z podziałem na role
    - SSL VPN dla nieograniczonej liczby użytkowników
    - Secure browser-only access (CVPN)
    - ICA proxy do XenApp
    - Integracja z Citrix StoreFront

3. Wsparcie dla następujących metod uwierzytelniania użytkowników
    - Lokalna – bez odwoływania się do zewnętrznych systemów

- certyfikatów cyfrowych
- LDAP
- SAML 2.0 - Security Assertion Markup Language
- Kerberos
- RSA SecureID
- Radius
- TACACS - Terminal Access Controller Access-Control System

4. Bezpieczeństwo
   - Filtrowanie zawartości HTTP/HTTPS
   - Zabezpieczenie przed przeciążeniem serwera, do którego skierowane jest żądanie
   - Wsparcie dla DNSSEC
   - Zabezpieczenie przed atakiem DoS, w tym dla http

5. System musi mieć dostępne co najmniej następujące metody równoważenia obciążenia
   - Najmniejsza liczba połączeń
   - Cykliczna
   - Ważona
   - Najszybsza odpowiedź serwera
   - Najmniejsza liczba połączeń i najmniejszej średniej odpowiedzi serwera
   - Najmniejszego obciążenia danej usługi
   - Najmniejszej liczby pakietów
   - Danych z monitora obciążenia
   - Rozkład ruchu pomiędzy serwerami aplikacji Web

6. Możliwość przekierowywania żądań wysyłanych do tego samego serwer WWW do różnych serwerów w zależności od zawartości (*Content Switching*) w oparciu o:
   - Domenę
   - Adres URL
   - Zdefiniowaną regułę
   - Typ urządzenia z którego nawiązywane jest połączenie
   - Cookie
   - Metodę HTTP
   - Źródłowy/docelowy adres IP, port
   - Content Switching musi być realizowany co najmniej dla następujących protokołów: HTTP, HTTPS, TCP i UDP

7. Utrzymywanie sesji (*session persistance* oraz stickiness) dla protokołów: HTTP, HTTPS, SIP,RTSIP,TCP/UDP, SSL. Wymagane mechanizmy przywiązywania sesji:
   - cookie
   - adres źródłowy
   - adres docelowy
   - identyfikator sesji SSL
   - SESSIONID
   - SIP call ID
8. Wsparcie dla usług warstw 4-7
   - inspekcja warstwy 7
   - wstrzykiwanie (*injection*) nagłówków http
   - ukrywanie zasobów
   - zmiana odpowiedzi serwera

- obsługa zaszyfrowanych cookies
- przepisywanie odpowiedzi (*response rewriting*)
- ochrona przed atakami DoS/DDoS i SYN Flood
- multipleksacja połączeń http
- kompresja i cache'owanie http
- Źródłowy NAT dla adresów VIP i dla farm serwerów

9. Rozwiązanie musi zapewniać globalne, inteligentne równoważenie obciążenia wykorzystując usługę DNS, jako mechanizm rozdziału ruchu (Global Server Load Balancing), w ramach, którego zapewni:

a. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI

b. Rozdzielanie ruchu korzystając, co najmniej z metod:

- Cykliczna
- Ważona
- Obciążenia serwera
- Najmniejszej liczby połączeń

c. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera DNS klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji
d. Wsparcie dla DNSSEC
e. Konwersja rekordów między IPv4 i IPv6
f. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji
g. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji

10. Firewall aplikacyjny będący integralną częścią każdego urządzenia i posiadający właściwości:

- Możliwość pracy w trybie hybrydowym rozumianym jako jednoczesne używanie negatywnego i pozytywnego modelu bezpieczeństwa
- Zgodny z OWASP 10
- Certyfikacja ICSA lab
- Zgodny z PCI DSS (Payment Card Industry Data Security Standard)
- Wsparcie dla XML
- Tryb uczenia się
- DNS firewall
- Wsparcie dla DDoS L4 - L7
- Wsparcie dla narzędzi skanujących bezpieczeństwo firm trzecich
- Logowanie ataków w warstwie aplikacji
- Powiadamianie poprzez e-mail w przypadku ataku

11. System musi posiadać co najmniej następujące interfejsy administracyjne:

- GUI przy wykorzystaniu protokołu https,
- zarządzanie poprzez SSH,
- zarządzanie poprzez API REST,

12. System musi posiadać następujące funkcje zarządzania:

- obsługa protokołu SNMP v1/v2c/v3,
- zewnętrzny syslog,
- zbieranie danych i ich wyświetlanie,
- zbieranie danych zgodnie z ustawieniami administratora,
- osobny adres dla interfejsu zarządzającego,

Tabela 2 UPS rackowy do urządzeń

Lp.	Parametr	Wymagania minimalne
1.	Nominalne napięcie wyjściowe (V)	230V AC
2.	Częstotliwość wejściowa (auto sensing)	50/60 Hz + / - 3 Hz
3.	Moc rzeczywista:	1500 VA / 1000W
4.	Gniazda wyjściowe	4 x IEC 320 C13\n2 x IEC Jumpers lub równoważne
5.	Zakres nominalnego napięcie wyjściowe	208-253V (230V)
6.	Czas ładowania	<3 godzin do pełnego naładowania
7.	Technologia UPS	Line-interactive
8.	Komunikacja i zarządzanie	
	Port USB	TAK
	Port szeregowy RS-232	TAK
	Port Ethernet	Moduł umożliwiający zarządzanie, monitoring oraz diagnostykę poprzez sieć
	Ochrona przed przepięciami i filtracja	TAK
9.	Czas podtrzymania w zależności od obciążenia - przewidywany okres, w którym UPS będzie działać wyłącznie na baterii	min 7 minut przy 100 % obciążeniu
10.	Wysokość (podana w jednostkach EIA)	2U (bez modułu rozszerzeń)
11.	Zaświadczenia	Certyfikaty : CE, CSA, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, TUV, VDE, REACH, PEP, EOLI, EnergyStar Zgodność z RoHS

Przed przystąpieniem do wdrożenia Wykonawca powinien wykonać poniższe czynności:

1. Przeprowadzenie analizy przedwdrożeniowej obejmującej weryfikację konfiguracji sieci Zamawiającego oraz analizę konfiguracji i reguł obecnego systemu TMG niezbędną do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze,
2. Przygotowanie projektu technicznego na bazie przeprowadzonej analizy uwzględniających wymagania Zamawiającego przedstawione na spotkaniach roboczych i uwzględniających zakres zapytania,
3. Konfigurację urządzeń i oprogramowania zgodnie z uzgodnionym i zaakceptowanym przez Zamawiającego projektem technicznym.
4. Przygotowanie testów akceptacyjnych potwierdzających poprawne wdrożenie rozwiązania uwzględniające zapisy zaakceptowanego projektu.
5. Przeprowadzenie testów akceptacyjnych.
6. Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.

Zadanie 2. Dostawa i wdrożenie wyspecyfikowanego oprogramowania

Wykonawca dostarczy niżej wymienione oprogramowanie wraz z niezbędnymi licencjami na okres nie krótszy niż gwarancja obejmująca cały system.

- do realizacji systemu udostępniającego usługi forward Proxy

- do zarządzania i monitorowania całego powstałego systemu oraz analizy danych

A. Oprogramowanie do realizacji systemu udostępniającego usługi forward Proxy

Oprogramowanie do udostępniania i kontroli ruchu wychodzącego od użytkowników z wnętrza sieci statystyki do Internetu. Wymagane jest dostarczenie minimum dwóch instancji wirtualnych do realizacji funkcjonalności forward Proxy, niezależnych od dostarczanych urządzeń, ale posiadające jeden wspólny systemem zarządzania, monitoringu i analityki dla całego dostarczanego systemu.

Wymagane funkcjonalności:

- Obsługiwanie minimum 4 wirtualnych CPU
- Obsługiwanie minimum 4 GB pamięć RAM na vCPU
- Wydajność minimum 4 000 transakcje SSL/sek dla długości klucza 2048
- Przepustowość: SSL throughput - minimum 5 Gbps
- Możliwość uruchomienia na platformach wirtualizacyjnych, VMware ESX/ESXi, Microsoft Hyper-V
- Forward proxy dla całego wychodzącego ruchu
- Explicit i transparent proxy

- Możliwość wglądu w zaszyfrowaną transmisję
- Polityki obejścia i przejmowania sesji SSL (*SSL interception bypass policies*)
- Dozwolone i zabronione listy URL
- Autentykacja i autoryzacja użytkowników co najmniej przez: domenę AD, certyfikaty cyfrowe
- Zarządzanie certyfikatami
- Wsparcie dla TLS 1.2, TLS 1.1, TLS 1.0

B. Oprogramowanie do zarządzania i monitorowania całego powstałego systemu oraz analizy danych

Wymagane jest dostarczenie jednego, spójnego systemu zarządzania i monitorowania powstałego środowiska posiadającego funkcjonalności:

- Nowe wersje i poprawki bezpieczeństwa w okresie gwarancyjnym
- Dla minimalnie 100 zarządzanych wirtualnych adresów IP (VIP) dla serwerów wirtualnych lub aplikacji
- Scentralizowane zarządzanie wszystkimi elementami
- Dostępna możliwość zainstalowania oprogramowania na maszynie wirtualnej w środowiskach XenServer, ESX, HyperV
- Oprogramowanie musi umożliwiać kontrolę dostępu opartą na rolach (RBAC).
- Oprogramowanie musi centralnie zarządzać wszystkimi modułami równoważenia obciążenia oraz być w stanie analizować informacje z modułu równoważenia obciążenia
- Oprogramowanie musi być w stanie zidentyfikować stan usługi oraz mieć możliwość poinformowania administratorów o ewentualnych problemach
- Oprogramowanie musi być w stanie dostarczyć informacje na temat aplikacji/usługi, a w szczególności stanu równoważenia obciążenia, adresu URL, liczby żądań, nazwy domeny, stanu odpowiedzi, adresu IP użytkownika, adresu IP serwera, systemu operacyjnego i agenta użytkownika.
- Oprogramowanie powinno umożliwić pokazanie listy typów ataków i adresów IP, z których jest najwięcej ataków oraz powinno być w stanie tworzyć wskazówki bezpieczeństwa dla aplikacji i być w stanie dostarczyć informacje na temat poziomu zastosowanego ataku i poziomu bezpieczeństwa.
- Oprogramowanie musi być w stanie dostarczyć informacje na temat opóźnienia: RTT, WAN Delay, serwer/użytkownik oraz IP użytkownika i kraju z którego użytkownicy uzyskują dostęp do aplikacji. Muszą one również zawierać typ sesji, wartości opóźnień, przepustowość, adresy IP użytkowników i serwerów, nazwę aplikacji i informacje o kanale dla każdego użytkownika.
- Oprogramowanie powinno mieć możliwość wyświetlania informacji protokołu SSL pogrupowanych zgodnie z kluczowymi właściwościami certyfikatów oraz komunikować upływ ważności certyfikatów przez e-mail lub SMS
- Oprogramowanie musi obsługiwać integrację z VMware NSX.

Przed przystąpieniem do wdrożenia oferowanego oprogramowania należy wykonać projekt techniczny uwzględniający wymagania Zamawiającego przedstawione na spotkaniach roboczych oraz wymagania zapisane w OPZ.

Po wykonaniu wdrożenia należy wykonać dokumentację powykonawczą opisującą szczegółową konfigurację wdrożonego rozwiązania.

Zadanie 3. Przeniesienie usług obecnie pracujących na systemie TMG na nowy system

Przeniesienie usług obecnie pracujących na systemie TMG obejmować będzie:

- Opracowanie zaleceń dotyczące konfiguracji sieci, w szczególności dotyczące obecnej strefy DMZ prowadzonej przez TMG
- Opracowanie reguł dotyczących filtrowania ruchu sieciowego na urządzeniach brzegowych (firewall'ach) jeżeli będą wymagane.
- Wykonanie integracji Systemu publikacji usług do Internetu z Active Directory w szczególności w zakresie możliwości uwierzytelniania użytkowników korzystających z usług publikowanych do Internetu.
- Przeniesienie istniejących reguł publikujących usługi oraz reguł pomocniczych (jeżeli będą wymagane) z systemu TMG 2010 na dostarczony System publikacji usług do Internetu
- Produkcyjne uruchomienie przeniesionych usług na dostarczonym Systemie publikacji usług do Internetu
- Uruchomienie usługi VPN
- Przeniesienie obecnego ruchu wychodzącego na dostarczony system
- Rekonfiguracja proxy na urządzaniach końcowych za pomocą protokołu wpad
- Utworzenie zestawu reguł i raportów – do oprogramowania zarządzającego, minimalny zestaw musi obejmować: zestawienie zbiorcze dzienne, zestawienie rodzajów usług, listę adresów url, zestawienie użytkowników.

Zadanie 4. Realizacja szkolenia

1. Wykonawca przeprowadzi **5 dniowe szkolenie dla 4 administratorów** systemu zgodnie z następującymi wymaganiami:

    a. Program szkolenia – instalacja i konfiguracja komponentów wdrożonego rozwiązania ze szczególnym uwzględnieniem konfiguracji poszczególnych elementów sprzętowych i programowych w tym szczegółowe omówienie sposobu i metod udostępniania usług do Internetu.

    b. Szkolenie musi mieć formę wykładów i warsztatów.

    c. Wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF.

    d. Wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia i posiadania odpowiednich kompetencji administratora.

    e. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz zakwaterowaniem uczestników kursu jeśli szkolenie będzie odbywać się poza Warszawą.

    f. Wykonawca każdego dnia trwania szkolenia zapewni wyżywienie dla wszystkich uczestników: dwie przerwy kawowe, każda trwająca ok. 10 minut oraz jedną przerwę obiadową trwającą ok. 40 minut.

    g. W przypadku szkoleń poza Warszawą Wykonawca zapewni uczestnikom szkolenia - 3 posiłki dziennie, w tym śniadanie, obiad, kolacja oraz napoje i drobne

przekąski w czasie przerw (kawa, herbata, woda mineralna), w przypadku szkoleń w Warszawie – 1 ciepły posiłek (obiad) oraz napoje i przekąski w czasie przerw.

h. Wykonawca pokryje wszelkie koszty związane z dojazdem, pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

2. Do 14 dni od daty podpisania Umowy Wykonawca przedstawi Zamawiającemu do akceptacji – program i termin szkolenia przygotowany w porozumieniu z Zamawiającym.

3. Wykonawca zobowiązany będzie do przeprowadzenia szkolenia zgodnie z zatwierdzonym przez Zamawiającego szczegółowym zakresem tematycznym i harmonogramem.

4. Wykonawca w ramach prowadzonego szkolenia zobowiązany jest przekazać Zamawiającemu:

   a. materiały szkoleniowe,
   b. listę obecności,
   c. listę wydanych zaświadczeń i komplet imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenie, pod warunkiem uczestnictwa w pełnym wymiarze zajęć.