**Załącznik nr 1 do Umowy nr …… z dnia ……..**

**OPIS PRZEDMIOTU ZAMÓWIENIA – część 3**

**§1**

Przedmiotem zamówienia jest:

* 1. świadczenie przez Wykonawcę usług serwisu pogwarancyjnego, obejmujących usuwanie zgłoszonych awarii i usterek dla sprzętu oraz oprogramowania Zamawiającego wymienionych poniżej jako **„Infrastruktura sprzętowa posiadana przez Zamawiającego”**, a w razie konieczności jego wymianę oraz wykonanie innych czynności określonych w § 2,
  2. świadczenie usługi wsparcia technicznego (asysty technicznej) w liczbie roboczogodzin określonej w niniejszym Załączniku,
  3. przeprowadzenie warsztatów szkoleniowych z zakresu merytorycznego określonego w niniejszym Załączniku.
  4. udzielenie lub zapewnienie udzielenia niezbędnych licencji na oprogramowanie wskazane w niniejszym Załączniku.

**§ 2**

1. Wykonawca zobowiązuje się świadczyć usługi serwisu w miejscu użytkowania sprzętu, z możliwością naprawy w serwisie Wykonawcy, jeżeli naprawa sprzętu w miejscu użytkowania okaże się niemożliwa. W przypadku braku możliwości dokonania naprawy w miejscu użytkowania sprzętu i konieczności jego dostarczenia do punktu serwisowego wskazanego przez Wykonawcę, koszty dostarczenia uszkodzonego sprzętu do punktu serwisowego oraz   
   z punktu serwisowego do miejsca użytkowania pokrywa Wykonawca.
2. Wykonawca zobowiązuje się do ponoszenia wszelkich kosztów naprawy sprzętu, w tym kosztów części zamiennych i podzespołów transportu, instalacji, konfiguracji i uruchomienia sprzętu.
3. Wykonawca zobowiązuje się do świadczenia usług serwisu z należytą starannością z uwzględnieniem ogólnie przyjętych i stosowanych standardów   
   i procedur przy tego rodzaju usługach, a także zaleceń lub procedur określonych przez producentów sprzętu.
4. Nośniki informacji takie jak, np. dyski twarde, pamięci flash, mogą być naprawiane jedynie w miejscu ich użytkowania, a w przypadku konieczności wymiany uszkodzonych nośników na nowe, wolne od wad, nośniki informacji pozostają u Zamawiającego. W przypadku konieczności dokonania naprawy sprzętu wyposażonego w nośniki informacji poza miejscem użytkowania, nośniki pozostają w siedzibie Zamawiającego.
5. Wykonawca zobowiązany jest do dostarczenia Zamawiającemu niezbędnych danych do autoryzacji na stronie www producenta w celu pobierania nowych wersji oprogramowania sprzętu, poprawek, korzystania z bazy wiedzy, instrukcji obsługi itp.
6. Wykonawca zobowiązuje się przyjmować zgłoszenia serwisowe poprzez stronę www Wykonawcy dostępną przez całą dobę, 365 dni w roku. Wykonawca dostarczy dane niezbędne do autoryzacji na stronie www Wykonawcy w celu dokonywania zgłoszeń serwisowych przez Zamawiającego. Zamawiający wymaga również zapewnienia możliwości dokonywania zgłoszeń serwisowych poprzez e-mail na adres ............@............ w przypadku braku możliwości dokonania zgłoszenia serwisowego przez stronę www (np. w przypadku braku dostępności dedykowanej strony www). Wzór Formularza zgłoszenia serwisowego będzie stanowił załącznik do umowy. Wykonawca potwierdzi otrzymanie zgłoszenia serwisowego poprzez wysłanie wiadomości e-mail na adres ............@............ .Wszelkie wykonane przez Wykonawcę lub jego przedstawicieli czynności serwisowe wymagają dokumentowania w formie pisemnej.
7. W przypadku, jeżeli naprawa wymaga wymiany urządzenia Zamawiający wymaga, aby Wykonawca każdorazowo w takiej sytuacji przedstawił informacje w tym zakresie przedstawicielowi Zamawiającego do akceptacji. Zamawiający zobowiązany jest do udzielenia odpowiedzi w terminie nie dłuższym niż 30 minut. Brak odpowiedzi w wyżej wymienionym terminie oznacza akceptację.
8. Wykonawca zobowiązuje się, że nie będzie dokonywał żadnych modyfikacji sprzętu bez wcześniejszego uzgodnienia ich z Zamawiającym. Zamawiający zobowiązany jest do udzielenia odpowiedzi w terminie nie dłuższym niż 30 minut. Brak odpowiedzi w wyżej wymienionym terminie oznacza akceptację. Zamawiający zastrzega sobie prawo do samodzielnej rozbudowy sprzętu i dokonywania zmian w konfiguracji..
9. Wykonawca zobowiązany jest do świadczenia serwisu pogwarancyjnego na każde zgłoszenie serwisowe Zamawiającego.
10. Czas usunięcia awarii lub usterki liczony jest w godzinach od momentu wysłania przez Zamawiającego do Wykonawcy formularza „zgłoszenia serwisowego”.
11. Wykonawca podejmie działania serwisowe w trybie 24x7x365- zgłoszenie awarii lub usterki przez wszystkie dni tygodnia, 365 dni   
    w roku, naprawa urządzeń (z wyłączeniem awarii oprogramowania) w ciągu 4 godzin od przesłania zgłoszenia przez Zamawiającego w przypadku awarii oraz naprawa urządzeń (z wyłączeniem usterek oprogramowania) w ciągu …… godzin (zgodnie z ofertą Wykonawcy jednak nie dłużej niż 8 godzin) od przesłania zgłoszenia przez Zamawiającego w przypadku usterki.
12. Zamawiający dopuszcza możliwość usunięcia awarii lub usterki poprzez dostarczenie i uruchomienie sprzętu zastępczego z zachowaniem terminów określonych w ust. 11. Wykonawca zobowiązany jest do dostarczenia w tym terminie Zamawiającemu kompatybilnego sprzętu zastępczego, wolnego   
    od wad, o parametrach wydajnościowych i funkcjonalnych nie gorszych niż sprzęt podlegający naprawie. Wykonawca zobowiązuje się jednocześnie   
    do naprawy uszkodzonego sprzętu i jego konfiguracji, instalacji i uruchomienia (zamiast sprzętu zastępczego) w terminie nie dłuższym niż 30 dni od przesłania zgłoszenia serwisowego.
13. Wykonawca zobowiązany jest w dniu wykonania naprawy do potwierdzenia wykonania naprawy na protokole „zgłoszenia serwisowego”.   
    Ww. dokument musi zostać podpisany (data, godzina i podpis) przez przedstawiciela Zamawiającego, Data i godzina podpisania ww. dokumentu   
    bez zastrzeżeń przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi naprawy.
14. W przypadku wystąpienia awarii tego samego elementu po wykonaniu 3 napraw w okresie obowiązywania umowy, Wykonawca zobowiązuje   
    się na pisemne wezwanie Zamawiającego do wymiany tego elementu na fabrycznie nowy, nieużywane i wolne od wad na sprawny, tego samego producenta i tego samego typu o parametrach wydajnościowych i funkcjonalnych nie gorszych niż element wymieniany w terminie 30 dni od dnia otrzymania od Zamawiającego wezwania do wymiany. Nowe elementy musza być wyprodukowane nie wcześniej niż sześć miesięcy przed terminem składania ofert.
15. W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z ust. 11 Zamawiający na koszt Wykonawcy ma prawo wypożyczyć od dowolnego Wykonawcy sprzęt zastępczy o nie gorszych parametrach od sprzętu ulegającego awarii, zachowując jednocześnie prawo do naliczenia kary umownej   
    i odszkodowania. Jednocześnie Zamawiający ma prawo zlecić dowolnej firmie naprawę uszkodzonego sprzętu, a kosztami naprawy obciążyć Wykonawcę, zachowując jednocześnie prawo do naliczenia kary umownej i odszkodowania, nie tracąc gwarancji Wykonawcy
16. W przypadku dokonania naprawy przez Wykonawcę poprzez wymianę elementów, zostaną zainstalowane fabrycznie nowe elementy o parametrach wydajnościowych i funkcjonalnych nie gorszych niż elementy wymieniane.
17. Po usunięciu awarii lub usterki, dostarczeniu sprzętu zastępczego lub wymianie na sprzęt nowy, wolny od wad, obowiązkiem Wykonawcy będzie również uruchomienie i odtworzenie konfiguracji sprzętu wraz z oprogramowaniem w miejscu użytkowania. Odtworzenie konfiguracji jest zależne od dostarczenia przez Zamawiającego kopi konfiguracji. Przekazanie kopi konfiguracji sprzętu do Wykonawcy nastąpi niezwłocznie.
18. Strony zobowiązują się do wzajemnego przekazywania sobie niezwłocznie wszelkich informacji mogących mieć wpływ na realizację zamówienia. Wykonawca niezwłocznie udzieli odpowiedzi w formie pisemnej na zgłaszane przez Zamawiającego uwagi dotyczące realizacji zamówienia, w terminie nie dłuższym niż 2 dni robocze.
19. Osoby wskazane przez Wykonawcę do realizacji umowy zobowiązane są do przestrzegania postanowień regulaminów wewnętrznych i stosowania odpowiednich procedur obowiązujących w Ministerstwie Sprawiedliwości. Osoby skierowane przez Wykonawcę do realizacji umowy zobowiązane   
    są do zapoznania się i stosowania się do zapisów polityki bezpieczeństwa Ministerstwa Sprawiedliwości. Powyższe zostanie potwierdzone pisemnym oświadczeniem każdej z osób wyznaczonych do realizacji umowy.
20. Wykonawca zobowiązany jest do dostarczenia wszelkich części zamiennych, podzespołów i materiałów, które są niezbędne do utrzymania sprzętu sieciowego i oprogramowania sprzętu sieciowego objętego umową w należytym stanie technicznym tj. fabrycznie nowe, nieużywane i wolne   
    od wad oraz, które są wymagane w ramach dostępnych i zalecanych ulepszeń technicznych.
21. Wykonawca zobowiązany jest do zapewnienia niezbędnych części i materiałów w ramach wynagrodzenia za wykonanie przedmiotu umowy.
22. W ramach serwisu pogwarancyjnego Wykonawca wykona aktualizację oprogramowania sprzętu objętego serwisem, nie rzadziej niż raz na 180 dni za pomocą aktualnych narzędzi aktualizujących do wersji uzgodnionej z Zamawiającym.
23. Harmonogram wykonania wszystkich aktualizacji oprogramowania sprzętu objętego serwisem pogwarancyjnym zostanie uzgodniony z Zamawiającym   
    w terminie do 30 dni przed przystąpieniem do ww. prac.
24. Przed przystąpieniem do prac związanych z aktualizacją oprogramowania sprzętu Wykonawca przeprowadzi analizę wpływu dokonywanej aktualizacji   
    na sprzęt podłączony do innego sprzętu i pozostałych urządzeń podłączonych do sprzętu sieciowego.
25. W przypadku wystąpienia problemów, ze sprzętem (lub wersją oprogramowania), a objętym serwisem pogwarancyjnym, wynikających   
    z przeprowadzonej aktualizacji oprogramowania sprzętu (lub brakiem komunikacji sieciowej z/do urządzeń podłączonych do sprzętu), Wykonawca niezwłocznie wykona powrót do poprzednich wersji i na własny koszt zapewni rozwiązanie problemów z urządzeniami, których prawidłową prace zakłóciły działania prowadzone przez Wykonawcę.

26. Wykonawca:

1. przeprowadzi, nie rzadziej niż jeden raz na 180 dni analizę w zakresie uaktualnień poziomu oprogramowania sprzętu sieciowego, poziomu firmware’u (mikrokodów);
2. przedstawi Zamawiającemu raport po wykonanej obsłudze serwisowej;
3. opracuje harmonogram prac optymalizacji instalacji uaktualnień;
4. zweryfikuje poprawność działania Sprzętu sieciowego i oprogramowania sprzętu sieciowego po wykonaniu obsługi serwisowej.

27. Wykonawca zobowiązany jest do zapewnienia dostępu dla Zamawiającego do dedykowanego portalu www producenta dla urządzeń, na którym będzie możliwe co najmniej pobieranie nowych wersji dedykowanego dla danego urządzenia oprogramowania, pobieranie aktualizacji, patch-y, a także dostęp do baz wiedzy, przewodników konfiguracyjnych, narzędzi diagnostycznych, oprogramowania wspomagającego, itp.

28. Zamawiający wymaga zapewnienia dostępu do pomocy technicznej Wykonawcy i producenta oraz do zasobów pobierania oprogramowania do urządzeń objętych serwisem. Wykonawca musi zapewnić Zamawiającemu dostęp do najnowszego oprogramowania do urządzenia objętego serwisem pogwarancyjnym. Wykonawca jest zobligowany do instalowania najnowszego oprogramowania na urządzeniach oraz zapewnienia ciągłości działania sprzętu.

29. W ramach umowy na żądanie Zamawiającego Wykonawca podniesie wersje oprogramowania na dwóch urządzeniach do aktualnej wersji wraz   
z niezbędnymi poprawkami, tzw. Hotfix.

**Infrastruktura sprzętowa posiadana przez Zamawiającego:**

**Urządzenia bezpieczeństwa**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa urządzenia** | **Moduł** | **Numer seryjny** | **Miejsce instalacji** |
| 1 | Check Point 12600 | CPAP-SG12600-NGTP | 1345B02105 | MS  Warszawa  ul. Czerniakowska 100 |
| WDC WD5003ABYZ-011FA0 |  |
| WDC WD5003ABYZ-011FA0 |  |
| NIP-51081-090 |  |
| NIP-51040-090 |  |
| CPAP-ACC-2-10F |  |
| Memory Slot od 1 do 12 - Size: 1024 |  |
| Power Supply #1 |  |
| Power Supply #2 |  |
| CPSB-NGTP-12600-3Y |  |
| 2 | Check Point 12600 | CPAP-SG12600-NGTP | 1345B02099 | MS  Warszawa  ul. Czerniakowska 100 |
| WDC WD5003ABYZ-011FA0 |  |
| WDC WD5003ABYZ-011FA0 |  |
| NIP-51081-090 |  |
| NIP-51040-090 |  |
| CPAP-ACC-2-10F |  |
| Memory Slot od 1 do 12 - Size: 1024 |  |
| Power Supply #1 |  |
| Power Supply #2 |  |
| CPSB-NGTP-12600-3Y |  |

**§ 3**

* + - 1. Wykonawca zapewni świadczenie usługi wsparcia technicznego inżyniera (asysty technicznej), zgodnie z potrzebami Zamawiającego, przez minimum dwóch inżynierów, którzy posiadają certyfikat na poziomie minimum Check Point Certified Security Expert (CCSE) R80 lub certyfikat równoważny. Osoby skierowane do realizacji zamówienia muszą posiadać aktualne certyfikaty w okresie obowiązywania umowy. Usługi wsparcia technicznego będą świadczone w wymiarze do 300 roboczogodzin (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę,   
         tzn. nie ma znaczenia ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny). Usługa będzie świadczona dla infrastruktury Zamawiającego (sprzętu i oprogramowania). Równoważność certyfikatów została opisana w SIWZ.
      2. Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym serwisem pogwarancyjnym. W przypadku, gdy Zamawiający zleci Wykonawcy prace, które powinny być zrealizowane w ramach serwisu pogwarancyjnego, Wykonawca ma obowiązek poinformowania o tym fakcie Zamawiającego.
      3. Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności rozwoju i modyfikacji sprzętu, zaawansowanej konfiguracji sprzętu oraz wsparcia w zakresie utrzymania sprzętu.
      4. Zamawiający będzie przekazywać Wykonawcy zlecenia w ramach asysty technicznej, w których określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
      5. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia wraz z rozbiciem na poszczególne czynności.
      6. Zamawiający może zaakceptować propozycję wykonania zlecenia albo odrzucić propozycję, co jest równoznaczne z nieudzieleniem zlecenia albo zażądać od Wykonawcy, w wyznaczonym terminie, dodatkowych wyjaśnień, informacji do przedstawionej propozycji wykonania zlecenia.
      7. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności:   
         zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, termin wykonania prac.
      8. Rozliczenie wsparcia technicznego inżyniera odbywać się będzie na podstawie podpisanych bez zastrzeżeń, przez Wykonawcę i Zamawiającego,   
         Miesięcznych Protokołów odbioru usługi.
      9. W ramach godzin wsparcia inżynier na wezwanie Zamawiającego ma obowiązek przybyć do wskazanego miejsca/siedziby na terenie Warszawy   
         i tam realizować zgłoszenie.

**§4**

* + - 1. Wykonawca przeprowadzi warsztaty szkoleniowe z zakresu merytorycznego oprogramowania Check Point. Warsztaty zostaną przeprowadzone   
         w ośrodku szkoleniowym na terenie Warszawy, po 4 cykle szkoleniowe dla 4 osób (w dwóch turach – po 2 osoby), w wymiarze po minimum   
         16 godzin zegarowych każdy cykl.
      2. Wykonawca zobowiązany jest do przeprowadzenia szkoleń w terminie do 24 miesięcy od daty zawarcia umowy.
      3. Każdy uczestnik szkolenia otrzyma certyfikat jego ukończenia.
      4. Szkolenia muszą być prowadzone w języku polskim.
      5. Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie szkoleń.   
         Wymagane jest, aby Kadra trenerska posiadała udokumentowane co najmniej 2 letnie doświadczenie w przedmiocie szkolenia.
      6. Wykonawca powinien dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazę szkoleniową z odpowiednimi pomieszczeniami wraz   
         z zapleczem do przeprowadzenia szkolenia dla osób dorosłych tj. sale dostosowane do prowadzenia zajęć, dobrze oświetlone (światło dzienne   
         i sztuczne), wentylowane (z dostępem do świeżego powietrza), posiadające odpowiednie warunki sanitarne, bezpieczeństwa i higieny pracy,   
         wyposażone w akustyczne i jakościowe narzędzia i urządzenia, a także oprogramowania i pomoce dydaktyczne niezbędne do wykonania zamówienia.
      7. W pobliżu sali wykładowej (w tym samym budynku) powinny znajdować się łazienki z węzłem sanitarnym.
      8. Program warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych warsztatów z podziałem na zajęcia teoretyczne i praktyczne.   
         Program powinien zawierać również informacje dotyczące wiedzy i umiejętności jakie zdobędą uczestnicy po zakończeniu warsztatów. Zamawiający   
         zastrzega sobie prawo do korekty programu warsztatów w zakresie nieograniczonym regulacjami prawnymi.
      9. Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy – z rozpisaniem na dni i godziny - oraz programy warsztatów   
         i dostarczy je do 7 dni roboczych przed realizacją zamówienia do akceptacji przez Zamawiającego. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.
      10. Zajęcia powinny odbywać się w dni powszednie od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin dziennie.   
          Harmonogram powinien zostać wydrukowany i rozdany uczestnikom szkolenia na pierwszym spotkaniu.
      11. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika do danego rodzaju szkolenia, pozwalające na samodzielną edukację   
          z zakresu tematyki szkoleń (opracowania, wydruki materiałów szkoleniowych).
      12. Komplet materiałów szkoleniowych dla każdego uczestnika szkolenia obejmuje:

a) papierową wersję materiałów szkoleniowych. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty   
w standardzie PDF, w miejsce materiałów papierowych;

b) materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne niezbędne do realizacji szkolenia.

13. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć.

14. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.

15. Wykonawca zapewni:

na potrzeby wyżywienia uczestników szkoleń odpowiednie pomieszczenie oraz niezbędną liczbę stołów i krzeseł. Zamawiający nie dopuszcza serwowania posiłków w tej samej sali, w której odbywają się szkolenia. Miejsce posiłku nie powinno być oddalone dalej niż 10 minut drogi pieszo od miejsca szkolenia; obiady powinny być zróżnicowane, dany zestaw obiadowy nie powinien powtarzać się częściej niż raz na 3 dni szkoleniowe; Wykonawca zapewni 2 przerwy kawowe podczas jednego dnia szkoleniowego

* + - 1. W zakresie wyżywienia uczestników szkoleń Wykonawca zapewni:

1. obiad dwudaniowy dla wszystkich uczestników szkolenia - (z opcją wegetariańską) obejmujące: zupę, gorące danie główne (mięsne   
   lub rybne) z dodatkami skrobiowymi oraz surówką/sałatkami, deser (wyroby cukiernicze lub owoce sezonowe), kawę i herbatę wraz   
   z dodatkami, wodę mineralną gazowaną i niegazowaną.
2. Wykonawca zapewni następujące gramatury wymienionych powyżej posiłków:

* zupa – co najmniej 0,25 l na uczestnika szkolenia,
* danie gorące (mięsne lub rybne, opcja wegetariańska - warzywne) – co najmniej 150 g na uczestnika szkolenia,
* zestaw surówek/sałatek – co najmniej 150 g na uczestnika szkolenia,
* dodatki skrobiowe - porcja ziemniaków lub frytek / makaronu / ryżu / kaszy – co najmniej 200 g na uczestnika szkolenia,
* kawa, herbata, woda mineralna gazowana i niegazowana - co najmniej 0,5 l na uczestnika szkolenia.

1. przerwa kawowa dla wszystkich uczestników szkolenia podczas jego trwania:

* serwis będzie dostępny przy sali szkoleniowej;
* naczynia, w których serwowany jest serwis kawowy powinny być szklane lub ceramiczne;
* Serwis kawowy dla każdego uczestnika szkolenia obejmuje:
* butelkowaną wodę mineralną gazowaną i niegazowaną (0,5 l);
* świeżo parzoną, gorącą kawę z ekspresu lub zaparzacza oraz kawę sypaną i rozpuszczalną;
* herbatę – co najmniej 3 rodzaje herbat w torebkach;
* dodatki – cukier, mleko do kawy, cytrynę;
* dodatki - np. ciastka / wafelki i inne słodycze oraz ciasto.
  + - 1. W zakresie wyżywienia Wykonawca zobowiązany jest do:

1. terminowego przygotowania i podania posiłków, zgodnie z ramowym programem szkolenia,
2. zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowaniu posiłków i ich podawaniu,
3. przygotowania posiłków zgodnie z zasadami racjonalnego wyżywienia, urozmaiconych z pełnowartościowych, świeżych produktów   
   z ważnymi terminami przydatności do spożycia,
4. przestrzegania w trakcie realizacji usług wchodzących w zakres przedmiotu umowy obowiązujących przepisów sanitarnych, w tym ustawy   
   z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia. (Dz.U.2015.594 j.t. z późn. zm.).

c) Czas na przerwy kawowe i obiadowe należy doliczyć do założonej liczby godzin szkolenia.

16. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.

17. Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego protokół odbioru warsztatu wraz   
z dołączonymi załącznikami tj. oryginalną listą obecności, harmonogramem i programem warsztatu oraz ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.

**Cykl szkoleniowy nr 1 - Zakres szkolenia/warsztatów**

* + zarządzanie bezpieczeństwem;
  + wprowadzenie do technologii Check Point;
  + zarządzanie polityką bezpieczeństwa;
  + warstwy polityki bezpieczeństwa;
  + produkty Check Point Security i ich licencjonowanie;
  + wizualizacja ruchu;
  + podstawowe pojęcia VPN;
  + zarządzanie dostępem użytkowników;
  + praca z Cluster XL;
  + praca z portalem gaia;
  + instalacja i zapoznanie się z smart console;
  + modyfikacja istniejącej polityki bezpieczeństwa;
  + inspekcja https;
  + konfiguracja dynamicznego i statycznego NAT;
  + zarządzanie dostępem administracyjnym;
  + instalacja i zarządzanie zdalnym security gateway;
  + zarządzanie kopiami zapasowymi;
  + definiowanie warstw polityki dostępu;
  + implementacja kontroli aplikacji i filtracji url;
  + defining and sharing security policy layers;
  + aktywacja compliance software blade;
  + praca z licencjami i kontraktami;
  + Praca z logami Check Point;
  + Utrzymanie logów Check Point;
  + Konfiguracja “Site-to-Site” VPN pomiędzy Alpha i Bravo;
  + Zapewnienie dostępu użytkowników;
  + Praca z Cluster XL;
  + Verifying Network Compliance;
  + Praca z CPView.

**Cykl szkoleniowy nr 2 - Zakres szkolenia/warsztatów**

* zaawansowane możliwości systemu GAIA;
* zawansowany firewall;
* automatyzacja i instrumentacja;
* zaawansowany clusterxl;
* klastry vrrp;
* optymalizacja i akceleracja securexl;
* akceleracja wielokorowa corexl;
* kolejkowanie ruchu;
* produkt smartevent;
* identyfikacja zdarzenia;
* monitorowanie sieci;
* badanie zdarzeń bezpieczeństwa;
* usuwanie skutków zdarzeń bezpieczeństwa;
* raportowanie zdarzeń bezpieczeństwa;
* środki zapobiegawcze;
* przykład smartevent;
* środowisko wysokiej dostępności;
* oprogramowanie mobile access software blade;
* wdrożenie mobile access;
* wybór rozwiązania zdalnego dostępu;
* opcje zdalnego dostępu;
* Check Point capsule;
* polityka dostępu mobilnego;
* zagrożenia;
* systemy wykrywania włamań (ips);
* antywirus;
* Anti-Bot;
* technologia “sandbox”;
* SandBlast – ochrona przed “Zero-Day”;
* wdrożenie SandBlast;
* opcje wdrożenia SandBlast;
* zapobieganie zagrożeniom mobilnym;
* uaktualnienie sms do wersji R80.10;
* wgrywanie Check Point hotfix;
* konfiguracja nowego klastra firewall;
* bazowe komendy linii poleceń w administracji firewall;
* konfiguracja manualna NAT;
* zarządzanie obiektami za pomocą Check Point API;
* włączenie Check Point vrrp;
* wdrożenie zapasowego security management server;
* inspekcja chain modules;
* praca z Secure XL;
* praca z CoreXL;
* ocena zagrożeń przy pomocy SmartEvent;
* zarządzanie dostępem mobilnym;
* zrozumienie ochrony IPS;
* wdrożenie IPS Geo Protections;
* przegląd ustawień Threat Prevention i Protections;
* wdrożenie Threat Emulation i Threat Extraction.

**Cykl szkoleniowy nr 3 - Zakres szkolenia/warsztatów:**

* zaawansowany IPS;
* zarządzanie IPS;
* monitorowanie IPS;
* architektura IPS;
* optymalizacja IPS;
* diagnostyka IPS;
* wdrożenie IPS;
* wdrożenie “Geo Protection” w IPS;
* Check Point Advanced IPS;
* wykorzystanie profili w IPS;
* ręczna aktualizacja ochrony IPS (opcjonalnie);
* metody i możliwości diagnostyczne IPS;
* optymalizacja wydajności IPS;
* zaawansowana diagnostyka IPS.

**Cykl szkoleniowy nr 4 - Zakres szkolenia/warsztatów:**

* wprowadzenie do Threat Prevention;
* Threat Prevention – ThreatCloud;
* Threat Prevention – IPS;
* Threat Prevention – Anti-bot & Antivirus;
* integracja z User Directory;
* zrozumienie mechanizmów ochronnych IPS;
* wykorzystanie wbudowanej diagnostyki IPS;
* wdrożenie zabezpieczeń globalnych IPS (“Geo Protection”);
* przegląd ustawień i mechanizmów ochronnych “Threat Prevention”;
* praca z produktami “anti-Bot” i antywirus;
* wdrożenie Threat Emulation.

**§5**

1. Zamawiający wymaga dostarczenia licencji dla dwóch urządzeń Check Point 12600 pracujących w klastrze HA na okres trwania umowy spełniających następujące wymagania (Zamawiający nie dopuszcza możliwości łączenia okresów trwania licencji np. 3 lata + 1 rok).

1. Zamawiający wymaga dostarczenia licencji zapewniających poniższe funkcjonalności:
   * + - 1. **Anti-Virus**

Oprogramowanie musi wykrywać i usuwać wirusy, spyware i inne złośliwe oprogramowanie, bazując na sygnaturach, analizie zachowań i analizie heurystycznej.

* + - * 1. **URL Filtering**

Licencja umożliwiająca na posiadanym urządzeniu Check Point 12600 włączenie modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny.

* + - * 1. **Intrusion Prevention System IPS**

Licencja na oprogramowanie musi identyfikować zagrożenia, blokować niepożądane aktywności, zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet. Posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji, możliwość detekcji ataków i zagrożeń opartych na protokole IPv6.

* + - * 1. **Anti-Bot**

Oprogramowanie musi wykrywać komputery zainfekowane przez bot, zapobiegć uszkodzeniom poprzez blokowanie komunikacji z botami. Anti-Bot powinien umożliwiać wykrycie oraz blokadę podejrzanego zachowania w chronionych segmentach sieci. Wykrycie zdarzenia powinno opierać na wielowarstwowej analizie (połączenie reputacji adresów URL, IP czy DNS połączonych z analizą cech charakterystycznych dla botnetów. Baza musi być regularnie aktualizowana w sposób automatyczny

* + - * 1. **Anti-Spam and Email Security**

Kompleksowe zabezpieczenie poczty elektronicznej tj. zaawansowana ochrona antyspamowa, w tym ocena treści i reputacja IP.

Mechanizmy wykrywania wiadomości SPAM powinny być niezależne od języka i dodatkowo zawierać dane o reputacji adresu IP nadawcy w celu uniknięcia fałszywej klasyfikacji. Rozwiązanie powinno wspierać mechanizmy „Zero-hour” w celu wykrycia nieznanych zagrożeń. Anti-Spam i ochrona poczty e-mail musi korzystać z list blokowania potencjalnych zagrożeń.