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

**OPIS PRZEDMIOTU ZAMÓWIENIA – część 5**

Przedmiotem zamówienia jest zakup systemu ochrony poczty elektronicznej i komunikacji WWW   
dla Ministerstwa Sprawiedliwości, zwany dalej „systemem”.

W ramach realizacji zamówienia Wykonawca:

1. dostarczy system ochrony poczty elektronicznej i komunikacji www;
2. przeniesie na rzecz Zamawiającego własność systemu oraz urządzenia wchodzące w skład systemu
3. udzieli lub zapewni udzielenie niezbędnych licencji do prawidłowego działania systemu;
4. opracuje projekt wdrożeniowy obejmujący instalację i konfigurację systemu i integrację   
   z systemami obecnie funkcjonującymi u Zamawiającego;
5. uruchomi i dokona konfiguracji wszystkich urządzeń i oprogramowania w oparciu o założenia projektu wdrożeniowego oraz wykona dokumentację powykonawczą;
6. przeprowadzi szkolenia z zakresu funkcjonowania, administrowania dostarczonego systemu,
7. udzieli 36-miesięcznej gwarancji, w ramach której zapewni wsparcie techniczne i opiekę serwisową dla dostarczonego i uruchomionego systemu;
8. zapewni asystę techniczną eksperta.
9. **Założenia dla systemu:**
10. System będzie stanowił uzupełnienie systemu ochrony styku z Internetem dla najczęściej wykorzystywanych kanałów komunikacyjnych – poczta elektroniczna i www.
11. System obejmować będzie trzy fundamentalne filary ochrony:
    1. ochrona poczty elektronicznej przed spamem i wirusami,
    2. ochrona komunikacji web przed pobraniem złośliwego kodu,
    3. ochrona przed złośliwym oprogramowaniem z wykorzystaniem zaawansowanych metod analitycznych.
12. System zapewni ochronę ruchu pocztowego oraz pozwoli na uzyskanie większej ziarnistości ochrony dla komunikacji www.
13. System wprowadzi dedykowane narzędzia ochrony przed złośliwym oprogramowaniem (anti-malware) uwzględniające analizę wsteczną dla przesyłanych informacji.
    1. **System ochrony poczty**

|  |  |
| --- | --- |
| **Wymagania ogólne** | 1. Zamawiający wymaga dostawy całościowego rozwiązania ochrony poczty elektronicznej, które docelowo musi realizować następujące funkcje:    1. ochronę przed szkodliwą treścią (m.in. malware, wirusy etc.),    2. ochronę przed spamem,    3. filtrowanie treści przesyłanej w poczcie elektronicznej (w tym załączniki),    4. ochronę przed utratą informacji wrażliwych (wbudowany system DLP). 2. Zamawiający nie dopuszcza zaoferowania rozwiązania polegającego  na wykorzystaniu wyłącznie maszyn wirtualnych. System musi być oparty na dedykowanej platformie sprzętowej. 3. Rozwiązanie musi umożliwiać kontrolę protokołu SMTP w tym szyfrowane wersje tego protokołu: SSL i TLS. 4. System musi zapewniać filtrowanie poczty przychodzącej i wychodzącej, przy czym musi istnieć możliwość przypisana odrębnych polityk dla każdego z kierunków przesyłania poczty elektronicznej. 5. System musi zapewniać ochronę dla komunikacji z wykorzystaniem protokołu IPv4 i IPv6. 6. Rozwiązanie musi pracować jako gateway dla poczty elektronicznej (MTA - Mail Transfer Agent). |
| **Architektura rozwiązania** | 1. Rozwiązanie musi być dedykowanym MTA (Mail Transfer Agent) pracującym w trybie bramy dla przychodzącego i wychodzącego ruchu SMTP. 2. System musi umożliwiać tworzenie klastrów w trybie active-active  z rozkładem obciążenia. 3. System musi składać się z co najmniej dwóch redundantnych urządzeń potrafiących pracować zarówno w trybie aktywny-zapasowy jak  i aktywny-aktywny bez dodatkowych licencji wymaganych  do uruchomienia tych funkcjonalności. 4. Rozwiązanie musi wspierać protokoły SMTP, ESMTP, Secure SMTP over TLS, jako protokoły Mail Injection i Mail Delivery 5. System operacyjny musi posiadać specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej. 6. Konfiguracja urządzenia musi być możliwa przez:    1. Interfejs Web: HTTP i HTTPS,    2. CLI: przez SSH i telnet. 7. Urządzenie musi wspierać następujące mechanizmy kryptograficzne:    1. TLS: 56-bit DES, 168-bit 3DES, 128-bit RC4, 128-bit AES i 256-bit-AES,    2. DomainKeys Signing: 512-, 768-, 1024-, 1536- i 2048-bit RSA. |
| **Definiowanie polityk** | 1. System zarządzania politykami musi umożliwiać wielokrotne wykorzystywanie w regułach predefiniowanych elementów takich jak filtry i akcje. 2. System musi umożliwiać definiowanie co najmniej następujących akcji  (w ramach polityki):    1. dostarczenie wiadomości z wykonaniem dodatkowych akcji:       1. zmodyfikowanie tematu przesyłki,       2. usunięcie i/lub dodanie nagłówka X-header,       3. wysłanie kopii wiadomości pod wskazany adres lub adresy email;    2. zablokowanie wiadomości;    3. zapisanie wiadomości do wskazanej kolejki;    4. wysłanie powiadomienia. 3. System musi umożliwiać budowanie polityk i wyjątków od polityk, obejmujących wszystkie funkcjonalności produktu, niezależnie dla ruchu wychodzącego i przychodzącego z zastosowaniem co najmniej:    1. domen email,    2. obiektów z Microsoft AD,    3. adresów pojedynczych użytkowników. 4. System musi umożliwiać tworzenie odrębnych polityk i wyjątków dla różnych użytkowników. |
| **System ochrony antyspamowej** | 1. System powinien posiadać rozbudowane narzędzia zapobiegania przesyłaniu SPAM do serwera pocztowego. W tym celu system musi zapewniać mechanizmy ochrony oparte co najmniej o:    1. Sygnatury,    2. Słowniki,    3. Heurystykę, dla której musi być możliwa regulacja czułości (kontrola ilości False-Positives). 2. System musi posiadać wbudowane mechanizmy metody wykrywania wiadomości komercyjnych typu „Newsletters” i umożliwiać traktowanie tych wiadomości w zależności od ustalonej polityki organizacji jako SPAM lub jako wiadomość dopuszczona. 3. System musi zapewnić opcję definiowania wyjątków od stosowanych polityk. 4. Mechanizm antyspamowy musi być realizowany dwufazowo. 5. Pierwsza faza musi opierać się na sprawdzeniu reputacji adresu IP nadawcy w ogólnoświatowej bazie reputacji, która musi posiadać następujące parametry:    1. musi otrzymywać dane z co najmniej 100.000 źródeł danych  z całego świata,    2. musi analizować co najmniej 150 parametrów dotyczących ruchu poczty elektronicznej i protokołu WWW (w tym co najmniej 90 dla poczty),    3. musi zwracać wynik reputacji dla adresu IP w skali co najmniej 10-stopniowej czyli np. od 0 do 10,    4. system musi zwracać rezultat reputacji jedynie na podstawie zbieranych danych, nie dopuszczając jednorazowych interwencji ze strony wysyłających pocztę mających na celu manualne podwyższenie ich reputacji,    5. system musi umożliwiać wykorzystanie, co najmniej dwóch systemów badania reputacji nadawców dla poczty przychodzącej. Jeden z nich oparty o publiczny serwis Real-Time Blackhole List (RBL), drugi musi być systemem własnym producenta zaimplementowanym w rozwiązaniu. 6. Druga faza ma następować, jeżeli wiadomość przejdzie pomyślnie fazę pierwszą i musi opierać się na silniku antyspamowym, korzystającym z reguł otrzymywanych od producenta. 7. Reguły muszą być tworzone dynamicznie na podstawie informacji  z co najmniej trzech źródeł:    1. ogólnoświatowej bazy danych reputacji o parametrach jak w fazie pierwszej,    2. informacji zwrotnych od użytkowników proponowanego rozwiązania,    3. informacji od dedykowanych analityków bezpieczeństwa pracujących 24h na dobę, 7 dni w tygodniu, 365 dni w roku dla producenta proponowanego rozwiązania. 8. Reguły muszą weryfikować informacje na temat adresów IP pojawiających się w mailach jako linki do stron, strukturę wiadomości, sposób w jaki została wysłana, treść wiadomości  i reputację nadawcy. 9. Reguły powinny być uaktualniane, automatycznie, nie rzadziej niż  co 5 minut przez internet. 10. System musi posiadać możliwość skorzystania z funkcji reverse DNS lookup do określenia nazwy domeny dla adresu IP nadawcy wiadomości przychodzącej, wykonanie weryfikacji oraz odrzucenie połączenia  w przypadku:     1. braku rekordu PTR w DNS,     2. niezgodności nazwy domeny przesłanej w komunikacie SMTP HELO/EHLO z nazwą domeny w rekordzie DNS,     3. niezgodności rekordu reverse DNS (PTR) z rekordem forward DNS (A). 11. System musi umożliwiać weryfikację nadawcy wiadomości w oparciu  o mechanizm SPF (Sender Policy Framework). System powinien umożliwiać co najmniej:     1. odrzucenie lub przyjęcie wiadomości jeżeli rekord SPF nie istnieje,     2. odrzucenie wiadomości jeżeli rekord SPF nie pasuje do domeny nadawcy. 12. System musi umożliwiać: 13. monitorowanie i ograniczanie ilości połączeń z jednego adresu IP  w określonym przedziale czasu:     1. musi zapewniać opcję definicji przedziału czasowego,     2. musi zapewniać opcję ograniczenia maksymalnej ilości połączeń  i wiadomości. 14. ograniczanie maksymalnej liczby wiadomości przekazywanych  za pomocą pojedynczego połączenia SMTP. 15. wskazanie timeout’u dla niewykorzystywanego połączenia. 16. Rozwiązanie musi pozwalać na blokowanie na określony czas przyjmowania poczty z adresów IP, dla których odnotowano wiadomości zawierające zdefiniowaną liczbę niewłaściwych adresatów z chronionej domeny. |
| **System ochrony antywirusowej** | 1. System musi zapewniać blokowanie złośliwej treści:    1. z wykorzystaniem tradycyjnego skanowania antywirusowego opartego o co najmniej dwa komercyjne silniki antywirusowe oraz bazy sygnatur kodów złośliwych,    2. z wykorzystaniem zaawansowanych technik wykrywania zagrożeń jak metody oparte o heurystykę i analizy w czasie rzeczywistym,    3. musi zapewniać możliwość blokowania niebezpiecznych treści typu ActiveX, Javascript i VB script,    4. musi zapewniać mechanizmy reputacji i sandboxingu plików dla sprawdzenia informacji o przesyłanych obiektach w chmurze producenta w celu wykrywania i blokowania zagrożeń,    5. system musi umożliwiać definiowanie wyjątków od stosowanych polityk. 2. System musi mieć możliwość korzystania z co najmniej dwóch komercyjnych silników antywirusowych (na jednej platformie sprzętowej). 3. Silniki antywirusowe muszą korzystać z następujących metod skanowania wiadomości:    1. dopasowanie wzorców binarnych do sygnatur antywirusowych,    2. analiza heurystyczna,    3. emulacja uruchomienia kodu (w celu zapobiegania infekcji wirusami polimorficznymi). 4. Mechanizm musi mieć do dyspozycji oddzielną od dedykowanej dla spamu, kwarantannę, do której dostęp ma tylko administrator. 5. System musi zapewniać mechanizmy dynamicznej ochrony przed epidemią złośliwego kodu (ang. Outbreak):    1. mechanizm antywirusowy musi posiadać technologię umożliwiającą automatyczną kwarantannę wiadomości, które pomimo, że nie  są wskazane przez powyższe metody skanowania (z powodu  np. braku odpowiednich sygnatur antywirusowych), mogą jednak zawierać złośliwy kod,    2. informacje o takim podejrzeniu powinny być wysyłane przez globalną bazę reputacji, o parametrach opisanych w wymogach modułu antyspamowego,    3. podejrzane wiadomości powinny pozostać w kwarantannie,  aż do wypuszczenia przez producentów silników antywirusowych odpowiednich sygnatur i automatycznie wypuszczane i skanowane ponownie po ściągnięciu odpowiednich sygnatur. |
| **System ochrony przed złośliwym oprogramowaniem** | 1. System musi zapewniać mechanizmy zaawansowanej ochrony antimalware obejmujące:    1. sprawdzenie reputacji dla plików przesyłanych przez urządzenie,    2. kontrolę przesyłanych plików przez mechanizm sandboxingu  w chmurze,    3. monitorowanie wsteczne dla plików już przesłanych. 2. Kontrola reputacji dla plików musi odbywać się w ogólnoświatowej bazie reputacji. 3. Kontrola reputacji musi odbywać się na podstawie unikatowych metadanych własnościowych pliku, nie jest dopuszczalne, aby sprawdzenie reputacyjne wymuszało przesłanie pliku na zewnątrz systemu kontroli poczty. 4. Funkcja sandboxingu dla plików przesyłanych pocztą elektroniczną musi być wbudowana w system ochrony poczty, nie jest dopuszczalne stosowanie zewnętrznych systemów firm trzecich. 5. Funkcja monitorowania wstecznego musi umożliwiać informowanie administratora o zmianie decyzji dotyczących plików uprzednio przesłanych przez urządzenie. W szczególności dotyczy to sytuacji gdy we wskazanym pliku wykryto złośliwy kod. |
| **Filtrowanie  i kontrola treści** | 1. System musi umożliwiać kontrolę treści wiadomości co najmniej  w zakresie:    1. słowa kluczowe,    2. słowniki,    3. wyrażenia regularne,    4. typy załączników. 2. Kontrola musi obejmować co najmniej następujące elementy wiadomości:    1. tytuł,    2. treść,    3. nagłówki,    4. adres nadawcy,    5. adres odbiorcy. 3. Proponowane rozwiązanie musi posiadać mechanizmy analizy  i filtrowania oraz zarządzania treścią wiadomości poczty elektronicznej, zarówno treści samej wiadomości jak i jej załączników. 4. Mechanizm musi posiadać możliwość zdefiniowania polityki zarządzania treścią wiadomości w oparciu o wynik reputacji pobrany z bazy reputacji o parametrach opisanych w module antyspamowym. 5. Mechanizm musi posiadać możliwość zdefiniowania polityki zarządzania treścią wiadomości w oparciu o wynik uwierzytelnienia DKIM (Domain Keys Identified Messages), funkcjonalności opisanej w wymaganiach dotyczących zastosowania kryptografii w proponowanym rozwiązaniu. 6. Mechanizm musi posiadać możliwość filtrowania treści za pomocą integracji z zewnętrznymi słownikami. 7. System musi umożliwiać zarządzanie kolejkami (folderami) dla blokowanych wiadomości w zakresie zarządzania predefiniowanymi kolejkami oraz tworzenia nowych. 8. System musi zawierać moduł DLP umożliwiający identyfikację chronionych informacji z użyciem mechanizmów:    1. słowa kluczowe,    2. słowniki,    3. wyrażenia regularne,    4. właściwości przesyłanych plików takich jak prawdziwy typ pliku, jego nazwa lub rozmiar. 9. System musi zapewniać kwarantannę dla zablokowanych wiadomości. Dla kolejki kwarantanny musi być możliwe zdefiniowanie jej maksymalnej wielkości oraz czasu, po którym wiadomości będą usuwane. |
| **Kryptografia** | 1. Rozwiązanie musi posiadać mechanizmy oznaczania poczty wychodzącej (Bounce Address Tag Validation (BATV)) oraz weryfikacji tego oznaczenia w przypadku otrzymania wiadomości odbitej od odbiorcy (tzw. Bounce) w celu ochrony przed atakami typu „misdirected bounce spam”. 2. Rozwiązanie musi obsługiwać standard DKIM (Domain Keys Identified Messages) używany w celu uwierzytelnienia poczty, za pomocą szyfrowania asymetrycznego. 3. Rozwiązanie musi umożliwiać opcjonalnie, oddzielnie licencjonowanie, szyfrowanie symetryczne poczty dla wybranych wiadomości wykonywane bez potrzeby jakiejkolwiek ingerencji w klienta pocztowego oraz bez potrzeby implementacji PKI. Rozwiązanie powinno udostępniać szyfrowanie za pomocą algorytmów AES oraz RC4. |
| **Moduł raportujący i zarządzający** | 1. Konfiguracja urządzenia musi być możliwa poprzez:    1. Interfejs Web: HTTP i HTTPS,    2. CLI: przez SSH i telnet (w przypadku dedykowanego rozwiązania sprzętowego). 2. Rozwiązanie musi być wyposażone w system raportujący, umożliwiający:    1. generowanie predefiniowanych oraz własnych raportów na żądanie Zamawiającego oraz zgodnie z harmonogramem,    2. harmonogram powinien umożliwiać generowanie raportów codziennie, co tydzień i co miesiąc,    3. dostarczanie raportów w postaci plików pdf i csv,    4. dostosowanie tematu i treści automatycznie do wysyłanego maila zawierającego generowane raporty. 3. Zarządzanie, przeglądanie aktywności użytkowników oraz raportowanie muszą być dostępne przez zintegrowaną webową konsolę administracyjną. 4. Dostęp do webowej konsoli zarządzającej musi odbywać się przy użyciu bezpiecznego połącznia HTTPS. 5. Konsola zarządzająca musi zawierać ekran przedstawiający wykres sumarycznej aktywności z ostatnich 24 godzin oraz podstawowe statystki. 6. System musi udostępniać mechanizm pozwalający na przeglądanie przez chronionych użytkowników wiadomości umieszczonych w kwarantannie, umożliwiając im również zwolnienie wybranych wiadomości  z kwarantanny. |
| **Wymagane licencje** | 1. Proponowane rozwiązanie musi posiadać możliwość instalacji systemu na nieograniczonej liczbie maszyn wirtualnych. 2. Zaoferowane rozwiązanie musi posiadać licencje na czas nieokreślony na następujące funkcjonalności: MTA, DKIM, BATV i Filtrowania treści. 3. Proponowane rozwiązanie musi posiadać licencje dla ochrony 1500 skrzynek pocztowych na 3 lata (z możliwością ich przedłużenia) na następujące funkcjonalności:    1. antyspam,    2. antywirus z wykorzystaniem dwóch silników komercyjnych,    3. antiwirus z obsługą ochrony przed epidemią złośliwego kodu,    4. ochrona DLP,    5. szyfrowanie poczty,    6. zaawansowana ochrona przed złośliwym oprogramowaniem  z sandboxingiem dla plików – Anti-Malware. 4. Proponowane rozwiązanie musi zostać dostarczone z dedykowaną konsolą zarządzającą umożliwiającą centralne zarządzanie wszystkimi instancjami systemu ochrony poczty elektronicznej i www z jednego miejsca i spełniać szczegółowe wymagania dotyczące raportowania i zarządzania, opisane dla systemów ochrony poczty elektronicznej i www. 5. Dedykowana konsola zarządzająca musi zostać dostarczona w postaci dedykowanego urządzenia przystosowanego do docelowej obsługi 3000 użytkowników www i poczty elektronicznej. Jeżeli producent rozwiązania nie przewiduje dedykowanego sprzętu dla tego celu – i tylko w tym przypadku – należy dostarczyć stację roboczą/serwer w konfiguracji sprzętowej rekomendowanej przez producenta przy czym niedopuszczalne jest zaproponowanie konfiguracji minimalnej dopuszczonej przez producenta o ile nie jest to jedyna wytyczna przedstawiona przez producenta rozwiązania. |

**1.2 System ochrony komunikacji WWW**

|  |  |
| --- | --- |
| **Wymagania ogólne** | 1. System musi zapewniać ochronę dla komunikacji z wykorzystaniem protokołu IPv4 i IPv6. 2. System musi umożliwiać tworzenie klastra pracującego w trybie active-active z równoważeniem obciążenia na podstawie wag przypisanych do appliance z wykorzystaniem co najmniej WCCP oraz zewnętrznych sprzętowych load balancer’ów. 3. System musi posiadać możliwość działania jako proxy dla HTTP, HTTPS, FTP (ftp over http, ftp active, ftp passive). 4. System musi zapewniać możliwość działania jako:    1. proxy dedykowane (explicit proxy),    2. proxy transparentne (transparent proxy), z wykorzystaniem routingu opartego o polityki (PBR - policy based routing) lub przekierowania z wykorzystaniem protokołu WCCP v2. 5. System musi zapewniać możliwość współpracy z innymi serwerami proxy w konfiguracji hierarchicznych łańcuchów proxy (proxy chaining):    1. jako serwer nadrzędny, w trybie „upstream proxy” (parent proxy): 6. musi zapewniać możliwość użycia nagłówków informujących  o prawdziwym źródle połączenia (X-Auth-User oraz X-Forwarded-For), 7. jako serwer podrzędny, w trybie „downstream proxy” (child proxy);    1. musi zapewniać możliwość dodania nagłówków informujących  o prawdziwym źródle połączenia do zapytania URL (X-Auth-User oraz X-Forwarded-For). 8. System musi zapewniać możliwość nasłuchiwania obsługiwanych protokołów, na portach innych niż standardowe. 9. System ochrony web musi umożliwiać uwierzytelnienie użytkowników z wykorzystaniem mechanizmów NTLM i LDAP/Active Directory. 10. System musi posiadać możliwość integracji z Microsoft Active Directory w celu możliwości definiowania polityk dla użytkowników oraz innych elementów AD, w tym grup i OU. 11. System musi zapewniać możliwość lokalnego uwierzytelnienia użytkownika w przypadku braku informacji go identyfikujących. 12. System musi zapewniać cache’owanie obiektów pobieranych przez użytkowników (zmniejszenie wykorzystania pasma do Internetu). 13. System musi zapewniać wiele warstw ochrony, w tym:     1. pierwszą warstwą ochrony musi być sprawdzenie reputacji adresu IP bądź domeny, z którymi łączą się użytkownicy strefy chronionej, za pomocą danych zgromadzonych w globalnej bazie reputacji, która ustala reputację co najmniej w 10 stopniowej skali, np.  w zakresie od 0 do 10. Ocena reputacji musi być określana  na podstawie analizy co najmniej 50 różnych parametrów dotyczących adresów WWW co najmniej, takich jak:        * 1. weryfikacja, czy strona znajduje się na tzw. internetowych „Czarnych listach” stron WWW,          2. weryfikacja, czy strona znajduje się na tzw. Internetowych „Białych listach” stron WWW,          3. określenie w jakiej kategorii jest skatalogowana, wymaga się multikategoryzacji dla stron, co oznacza, że jedna strona może znajdować się w kilku kategoriach,          4. określenie treści strony,          5. sprawdzenia zachowania się URL podczas połączenia,          6. sprawdzenie danych dotyczących globalnego ruchu sieciowego dotyczącego tej strony,          7. sprawdzenie danych podmiotu na który domena jest zarejestrowana,          8. określenie czy adres IP strony pochodzi z puli adresów przydzielanych dynamicznie,          9. sprawdzenie czy adres znajduje się na liście serwerów  na które się włamano,          10. sprawdzenie danych właścicieli sieci, w których strona jest hostowana;     2. System musi umożliwiać rozróżnienie reputacji - oddzielnie dla obiektów na stronie www np. dla plików graficznych, java, flash itp. 14. System musi umożliwiać kontrolę ruchu użytkowników wewnętrznych do zasobów zewnętrznych na podstawie zdefiniowanych uprawnień. System musi zapewniać możliwość definiowania uprawnień dotyczących:     1. obiektu docelowego w oparciu o:        1. kategorię URL, do której przypisany jest dany adres URL,        2. adres IP zasobu,        3. wykorzystywany protokół lub aplikację.     2. Użytkowników wewnętrznych w oparciu o:        1. obiekty w Active Directory,        2. adresację IP. 15. System musi zapewniać ochronę przed niebezpieczną treścią w obu kierunkach ruchu pomiędzy siecią wewnętrzną i zewnętrzną. 16. System musi umożliwiać blokowanie złośliwej treści z wykorzystaniem:     1. skanowania antywirusowego,     2. zaawansowanych heurystycznych technik wykrywania. 17. System musi umożliwiać blokowanie dostępu do zasobów związanych  z zagrożeniami (malware, phishing, etc.). 18. System musi posiadać możliwość wykrywania i blokowania ruchu pochodzącego od zainfekowanych hostów wewnętrznych wychodzącego do Internetu (ruch typu Call Home do Botnet Command&Control). 19. System musi umożliwiać definiowanie granularnej polityki dostępu  do zasobów w określonych kategoriach URL z wykorzystaniem takich atrybutów jak:     1. nazwa użytkownika,     2. grupa użytkowników do której przynależy użytkownik,     3. adres IP stacji,     4. zakres adresów IP,     5. dzień tygodnia,     6. pora dnia. 20. System musi pozwalać na tworzenie własnych stron z komunikatami dla użytkowników. 21. System musi umożliwiać warunkowe udostępnianie użytkownikom, stron blokowanych przez aktualną politykę:     1. warunkowy dostęp może odbywać się poprzez wyświetlenie strony, na której użytkownik będzie mógł potwierdzić wolę skorzystania  ze strony pomimo iż jest to niezgodne z polityką,     2. warunkowy dostęp musi być definiowany przez administratora dla wybranych stron, adresów IP i obiektów na stronach,     3. informacja o decyzjach użytkowników muszą być zapisywane  w logach z dokładnością do informacji o:        1. czasie,        2. stronie do której dostęp był blokowany,        3. użytkowniku,        4. decyzji podjętej przez użytkownika. 22. System musi umożliwiać deszyfrację i inspekcję szyfrowanych połączeń HTTPS. 23. System musi zapewniać możliwość granularnej konfiguracji skanowania połączeń HTTPS w szczególności:     1. wyłączenie deszyfracji dla określonych kategorii stron internetowych,     2. wyłączenie deszyfracji dla wskazanych stron,     3. wyłączenie deszyfracji dla wskazanych adresów IP. 24. System pracujący w modelu proxy musi mieć możliwość kontroli atrybutów związanych z certyfikatem, przedstawianym przez serwer docelowy, w szczególności system musi:     1. weryfikować zgodność adresu zawartego w certyfikacie i żądanego przez użytkownika,     2. sprawdzać datę ważności certyfikatu,     3. zapewniać kontrolę łańcucha certyfikacji,     4. weryfikować unieważnienie certyfikatu z wykorzystaniem CRL oraz OCSP. 25. System musi zapewniać zarządzanie listą Trusted Root CA wykorzystywaną przy weryfikowaniu certyfikatów serwerów docelowych. 26. System powinien umożliwiać ostrzeganie użytkowników przed naruszeniem reguł z opcją kontynuacji. Zdarzenia takie muszą być logowane celem umożliwienia rekonfiguracji systemu i zdefiniowania dla nich domyślnych akcji w przyszłości. System musi umożliwiać zdefiniowanie co najmniej następujących akcji:     1. blokowanie,     2. blokowanie z możliwością kontynuacji,     3. wyłączenie inspekcji https dla danej strony. 27. System musi umożliwiać kategoryzację odwiedzanych przez użytkowników stron internetowych na podstawie ich bieżącej zawartości. 28. System musi zapewniać możliwość zdefiniowania procesu dynamicznej kategoryzacji dla stron, które nie są już skategoryzowane. Jednocześnie strony, które zostały uprzednio skategoryzowane nie będą podlegały ponownie temu procesowi. 29. System musi umożliwiać tworzenie polityki dostępu do zasobów internetowych w oparciu o:     1. słowa kluczowe zawarte w adresie URL,     2. typy plików,     3. zajętość pasma sieciowego dla streaming media. 30. System musi umożliwiać kontrolę nad działaniami użytkowników wykonywanych w ramach portali społecznościowych w tym korzystaniem z mikroaplikacji. Kontrola musi być możliwa  z granularnością dla funkcji w obrębie portali np. publikowanie komentarzy, zamieszczanie zdjęć, korzystanie z chat, etc. 31. System musi umożliwiać blokowanie aktywnych treści - ActiveX, JavaScript oraz Flash z treści dostarczanej użytkownikowi. 32. System musi umożliwiać tworzenie wyjątków dla poszczególnych stron internetowych, od obowiązującej polityki kontroli ruchu, niezależnie dla protokołów http, https i ftp lub aplikacji. Definicja wyjątków musi uwzględniać:     1. kategoryzację danej treści,     2. skanowanie zagrożeń,     3. usuwania treści aktywnych,     4. dostęp do protokołu i/lub aplikacji. 33. System musi pozwalać na elastyczne definiowanie ról administratorów z możliwością rozgraniczenia uprawnień. W szczególności system musi pozwalać na stworzenie roli z dostępem w trybie tylko do odczytu (Read-Only). 34. System musi umożliwiać przechowywanie logów dotyczących aktywności użytkowników przez okres zdefiniowany przez administratora. 35. System musi zapewniać narzędzie raportujące pozwalające na manualne oraz zautomatyzowane generowanie raportów w zakresie wszystkich parametrów monitorowanych i kontrolowanych przez system. 36. W szczególności raporty muszą obejmować:     1. analizę ruchu do konkretnych zewnętrznych adresów IP,     2. analizę ruchu do witryn internetowych oraz ich elementów,     3. analizę aktywności użytkowników wewnętrznych,     4. analizę aktywności wewnętrznych adresów IP. 37. System musi posiadać możliwość eksportowania raportów, co najmniej w formatach PDF oraz CSV. 38. System musi zapewniać możliwość informowania administratorów  o wystąpieniu określonych zdarzeń i incydentów w postaci wiadomości email wysyłanych na prekonfigurowane adresy poczty elektronicznej. 39. System musi zapewniać możliwość kontroli dostępu użytkowników  do poszczególnych raportów. 40. System musi umożliwiać filtrowanie protokołów wykrytych w ruchu sieciowym innym niż HTTP, HTTPS, FTP oraz tunelowanych  w HTTP/HTTPS. 41. System musi wykrywać i umożliwiać definiowanie reguł  dla następujących działań w sieci:     1. wykrywanie i kontrola nad transferem plików w sieci;     2. wykrywanie komunikatorów internetowych umożliwiających wymianę wiadomości w czasie rzeczywistym oraz przesyłanie plików/załączników,     3. wykrywanie i kontrola ruchu pomiędzy hostami w Botnet,     4. wykrywanie ominięcia lub podmiany serwera proxy,.     5. wykrywanie streamingu plików audio/wideo. 42. System musi posiadać możliwość filtrowania adresów URL. 43. System musi posiadać wbudowaną bazę adresów URL, z podziałem  na kategorie związane z treścią stron. Baza musi być utrzymywana przez producenta, aktualizowana i weryfikowana pod kątem poprawności zastosowanej dla stron www kategoryzacji. 44. System musi umożliwiać tworzenie własnych kategorii stron  i umieszczanie w nich stron nieskategoryzowanych jak też przynależących do innych kategorii. 45. System musi umożliwiać kategoryzację w czasie rzeczywistym witryn nieskategoryzowanych w bazie danych URL lub witryn należących  do kategorii dynamicznych (Social Networking i inne). 46. System musi umożliwiać analizę witryn internetowych z dokładnością do poszczególnych obiektów w szczególności w przypadku naruszenia polityki przez obiekt na stronie, wówczas użytkownikowi powinna zostać wyświetlona strona z pominięciem obiektów naruszających reguły. 47. System musi umożliwiać definiowanie następujących akcji w ramach filtrowania URL:     1. blokowanie,     2. dopuszczenie,     3. blokowanie z możliwością wejścia na stronę poprzez decyzję użytkownika o kontynuacji (wyświetlenie ostrzeżenia o naruszeniu polityki). 48. System musi umożliwiać definiowanie reguł dotyczących filtrowania URL z dokładnością do:     1. kategorii URL,     2. wskazanych URL w ramach dowolnej kategorii,     3. stron WWW,     4. określonych obiektów na stronie www,     5. treści typu ActiveX, Javascript lub Flash. 49. System musi zapewniać stosowanie filtracji opartych o reputację witryn i adresów IP. 50. System musi zapewniać blokowanie złośliwej zawartości jak szkodliwe oprogramowanie i wirusy z wykorzystaniem skanowania antywirusowego (silnik antywirusowy oraz bazy sygnatur malware). 51. System musi umożliwiać blokowanie złośliwej treści z wykorzystaniem zaawansowanych technik wykrywania zagrożeń jak metody behawioralne i analizy w czasie rzeczywistym. 52. System musi umożliwiać zastosowanie trzech komercyjnych silników antimalware jednocześnie. 53. System musi posiadać funkcję automatycznego wyboru i wykorzystania najlepszego silnika antymalware w zależności od rodzaju i typu treści przesyłanej w ramach strony www. System musi umożliwiać inspekcję równoległą – jednocześnie różnymi silnikami różnych obiektów strony. 54. System musi posiadać funkcję lokalnego sandboxingu lub badania  w chmurze w celu wykrywania i blokowania zagrożeń. 55. System musi zapewniać mechanizmy zaawansowanej ochrony antimalware obejmujące:     1. sprawdzenie reputacyjne dla plików przesyłanych przez urządzenie,     2. kontrolę przesyłanych plików przez mechanizm sandboxingu,     3. monitorowanie wsteczne dla plików już przesłanych. 56. Kontrola reputacji dla plików musi odbywać się w ogólnoświatowej bazie reputacji. 57. Kontrola reputacji musi odbywać się na podstawie unikatowych danych własnościowych pliku, nie jest dopuszczalne aby sprawdzenie reputacyjne wymuszało przesłanie pliku na zewnątrz systemu ochrony www. 58. Funkcja sandboxingu musi być realizowana bezpośrednio przez system ochrony www, nie jest dozwolone stosowanie zewnętrznych systemów firm trzecich. 59. Funkcja monitorowania wstecznego musi umożliwiać informowanie administratora o zmianie decyzji dotyczących plików uprzednio przesłanych przez urządzenie. W szczególności dotyczy to sytuacji gdy we wskazanym pliku wykryto złośliwy kod. 60. System musi posiadać możliwość definiowania wyjątków od stosowanej polityki, niezależnie dla każdego protokołu HTTP, HTTPS, FTP. 61. System musi być wyposażony w centralną webową konsolę zarządzającą umożliwiającą:     1. zarządzanie systemem,     2. przeglądanie aktywności użytkowników,     3. raportowanie. 62. System zarządzania rozwiązaniem musi zapewniać możliwość delegacji uprawnień do administrowania poszczególnymi składnikami i opcjami systemu. 63. System zarządzania musi umożliwiać zintegrowane zarządzanie rozwiązaniami tego samego producenta, również do ochrony poczty elektronicznej. 64. Dostęp do konsoli zarządzającej musi odbywać się z wykorzystaniem HTTPS i z weryfikacją uprawnień dostępu. 65. System musi umożliwiać delegowanie uprawnień do zarządzania  i raportowania. 66. System zarządzający musi udostępniać aktualne oraz historyczne dane dotyczące działania systemu. 67. Konfiguracja systemu ochrony www musi być przetrzymywana w pliku XML lub innym pozwalającym na jego przeglądanie w trybie offline. 68. System musi być wyposażony w moduł raportujący, umożliwiający:     1. generowanie raportów z podziałem na pojedynczych użytkowników, grupy użytkowników adresów IP i ich aktywności,     2. generowanie raportów z ukryciem danych pozwalających zidentyfikować użytkownika,     3. bieżący wgląd w aktywność użytkowników. 69. System musi umożliwiać monitorowanie aktywności użytkowników  co najmniej w oparciu o następujące kryteria:     1. adres URL,     2. kategoria adresu URL,     3. źródłowy adres IP,     4. docelowy adres IP,     5. port,     6. domena,     7. użytkownik,     8. akcja,     9. dzień,     10. wolumen przesłanych danych. 70. System musi umożliwiać integrację co najmniej w zakresie przekierowania ruchu z wykorzystaniem protokołu WCCP v2. 71. Rozwiązanie musi być zrealizowane w postaci dwóch dedykowanych urządzeń dostarczanych przez producenta systemu. 72. Rozwiązanie musi zostać posadowione na platformie sprzętowej  w konfiguracji 1U:     1. Procesor, minimum 6-rdzeniowymi,     2. pojemność dyskowa min. 2,4TB (RAID10) w tym dla potrzeb przechowywania logów,     3. minimum 32GB pamięci RAM,     4. redundancja zasilaczy (230V AC),     5. minimum 6 interfejsów Gigabit Ethernet, 73. Proponowane rozwiązanie musi być posadowione na redundantnych maszynach potrafiących pracować zarówno w trybie aktywny-zapasowy jak i aktywny-aktywny bez dodatkowych licencji wymaganych  do uruchomienia tych funkcjonalności. 74. System operacyjny musi posiadać specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi ochrony www. 75. System musi być przygotowany do pełnej obsługi 3000 użytkowników. 76. Proponowane rozwiązanie musi być zaoferowane z możliwością instalacji systemu na nieograniczonej liczbie maszyn wirtualnych. 77. Proponowane rozwiązanie musi posiadać licencje dla co najmniej 1500 użytkowników na 3 lata z możliwością przedłużenia o następujące funkcjonalności:     1. filtracja reputacyjna,     2. filtracja URL,     3. wykrywanie aplikacji i kontrola korzystania z www,     4. antymalware z wykorzystaniem trzech silników komercyjnych,     5. zaawansowana ochrona przed złośliwym oprogramowaniem  w wykorzystaniem analizy wstecznej – Anti-Malware. 78. Proponowane rozwiązanie musi zostać dostarczone wraz z dedykowaną konsolą zarządzającą umożliwiającą centralne zarządzanie wszystkimi instancjami systemu ochrony www i poczty elektronicznej (wirtualnymi i posadowionymi na dedykowanych urządzeniach) z jednego miejsca. 79. Proponowane rozwiązanie musi spełniać szczegółowe wymagania dotyczące raportowania i zarządzania opisane dla systemów ochrony poczty elektronicznej i www. 80. System musi być dostarczony z dedykowaną konsolą zarządzającą.     1. konsola musi zostać dostarczona w postaci oprogramowania  i dedykowanego urządzenia (appliance) przystosowanego  do docelowej obsługi 3000 użytkowników www i poczty elektronicznej,     2. jeżeli producent oferowanego rozwiązania nie przewiduje dedykowanego sprzętu dla tego celu dostarczając jedynie oprogramowanie zarządzające – i tylko w tym przypadku – należy dostarczyć stację roboczą/serwer pod konsolę zarządzania  w konfiguracji sprzętowej rekomendowanej przez producenta,     3. Zamawiający nie dopuszcza aby zaproponowana została sprzętowa konfiguracja minimalna dla konsoli zarządzania (opisana przez producenta oprogramowania jako minimalne wymagania dla oprogramowania zarządzającego), o ile nie jest to jedyna wytyczna przedstawiona przez producenta tegoż oprogramowania. |

**1.3 Dodatkowe wymagania:**

1. Oferowane produkty będą pochodziły z oficjalnego kanału dystrybucyjnego na terenie Unii Europejskiej.
2. Zamawiający wymaga, aby system i dostarczone w ramach systemu urządzenia były wolne od wad, fabrycznie nowe - bez śladów używania i bez uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Rzeczpospolitej Polskiej, wyprodukowane nie wcześniej niż 6 miesięcy od daty dostawy sprzętu, urządzenia muszą być dostarczone Zamawiającemu   
   w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, z załączonymi kartami gwarancyjnymi, dokumentami producenckimi i instrukcjami obsługi w języku polskim, a jeśli są one niedostępne to w języku angielskim. Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed   
   ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu realizacji procedur opisanych w zakresie Zamówienia, przy czym Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo uczestniczenia podczas czynności rozpakowywania.
3. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. najnowszej opublikowanej przez producenta) na dzień poprzedzający dzień składania ofert.
4. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta   
   do wycofania z produkcji lub sprzedaży.
5. Zamawiający musi mieć możliwość monitorowania statusu zgłoszeń serwisowych w systemie Wykonawcy i/lub producenta.
6. Zamawiający w ramach udzielonej gwarancji musi mieć możliwość zgłaszania awarii i zapytań   
   o pomoc techniczną zarówno do Wykonawcy, jak i bezpośrednio do producenta. Zamawiający wymaga obsługi nieograniczonej liczby zgłoszeń serwisowych. Zamawiający wymaga także, że w ramach serwisu gwarancyjnego uzyska bezpośredni dostęp do zasobów (bazy wiedzy) udostępnianych przez producenta.
7. Zamawiający informuje i wymaga, aby rozbudowa systemu nie powodowała utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia.
8. Wykonawca będzie realizował zgłoszenia awarii/usterek systemu w następujący sposób:

- awaria krytyczna, tj. niedostępność systemu dla wszystkich użytkowników: czas reakcji do 1 godziny od chwili zgłoszenia awarii przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do 4 godzin od chwili zgłoszenia awarii przez Zamawiającego;

- usterka (niepowodująca niedostępności systemu): czas reakcji do 1 godziny od chwili zgłoszenia usterki przez Zamawiającego, czas naprawy (przywrócenia funkcjonalności systemu) do 8 godzin od chwili zgłoszenia usterki przez Zamawiającego.

1. Obsługa zgłoszeń musi obejmować co najmniej:

* wymiany uszkodzonego sprzętu przez Wykonawcę,
* firmware upgrade/update – aktualizacja oprogramowania systemowego,
* dostęp do centrum pomocy technicznej producenta,
* dostęp do bazy wiedzy, dokumentacji i forum dyskusyjnego w ramach niepublicznych stron WWW producenta.

1. Wykonawca wykona wdrożenie systemu ochrony poczty oraz migrację konfiguracji z obecnie wykorzystywanego rozwiązania Microsoft TMG w sieci Zamawiającego – do nowego systemu ochrony WWW (rozwiązania), w ramach której wykonane zostanie:

* konfiguracja funkcji klastra na urządzeniach pozwalająca na logiczne połączenie dwóch urządzeń w jedno,
* migracja eksploatowanych obecnie połączeń fizycznych/logicznych do nowego systemu (rozwiązania),
* odwzorowanie i optymalizacja bieżącej konfiguracji na dostarczonym rozwiązaniu zgodnie   
  z najlepszymi praktykami producenta dostarczanego rozwiązania. Analiza obecnej konfiguracji urządzenia będącego w posiadaniu Zamawiającego (Microsoft TMG) w zakresie systemu ochrony WWW oraz rekonfiguracja zmian i implementacja nowych funkcjonalności na urządzeniu będącym przedmiotem zamówienia,
* konfiguracja systemu autoryzacji i uwierzytelniania, dodanie urządzeń oraz polityk dostępu,
* podłączenie wyspecyfikowanych urządzeń do istniejącej infrastruktury LAN Zamawiającego,
* wykonanie testów redundancji i niezawodności rozwiązania.

1. Czynności związane z uruchomieniem oraz migracją muszą być przeprowadzone przez personel Wykonawcy we współpracy z personelem IT Zamawiającego.
2. Dostawa musi obejmować wszystkie wymagane przez producentów oferowanego rozwiązania komponenty do jego prawidłowego podłączenia i konfiguracji w rozwiązaniu Zamawiającego takie jak między innymi: okablowanie, adaptery, wtyczki, listwy mocujące, urządzenia zasilające itp.(sieć energetyczna Zamawiającego o parametrach: 230 V ± 10%, 50 Hz).
3. Wykonawca zrealizuje liczbę godzin asysty technicznej eksperta do 400 roboczogodzin w zakresie przedmiotu zamówienia, określonego w pkt. 1.1 i pkt. 1.2 – Specyfikacji technicznej Opisu przedmiotu zamówienia,
4. W roboczogodzinę asysty technicznej eksperta nie wlicza się czasu dojazdu oraz ilości osób zapewniających wsparcie tzn. nie ma znaczenia ile osób będzie świadczyło asystę techniczną eksperta w danej roboczogodzinie/roboczogodzinach u Zamawiającego. Rozliczenie roboczogodzin wsparcia asysty technicznej eksperta odbywać się będzie miesięcznie   
   za faktycznie wykorzystane roboczogodziny na podstawie miesięcznych Protokołów odbioru asysty technicznej eksperta. Do godzin asysty technicznej eksperta nie wlicza się roboczogodzin usług wykonywanych na warunkach gwarancji.
5. Asysta techniczna eksperta będzie dotyczyła sprzętu/oprogramowania wyspecyfikowanego   
   w pkt. 1.1, 1.2 specyfikacji technicznej Opisu przedmiotu zamówienia. W ramach asysty technicznej eksperta Zamawiający nie będzie realizował aktualizacji firmware.
6. Zamawiający będzie przekazywać Wykonawcy zlecenia, w których każdorazowo określi przedmiot zlecenia oraz określi maksymalny, oczekiwany termin realizacji zlecenia.
7. Wykonawca w terminie wyznaczonym przez Zamawiającego, nie krótszym niż jeden dzień roboczy od otrzymania zlecenia, przekaże Zamawiającemu propozycję wykonania zlecenia zawierającą w szczególności wycenę prac zawartych w zleceniu, proponowaną liczbę roboczogodzin niezbędnych do wykonania zlecenia.
8. 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.
9. W przypadku akceptacji propozycji wykonania zlecenia Zamawiający przedłoży Wykonawcy zaakceptowane zlecenie zawierające w szczególności: zakres prac, liczbę roboczogodzin niezbędną do wykonania prac, kwotę wynagrodzenia należnego za zrealizowanie zlecenia, termin wykonania prac.
10. Rozliczenie wsparcia technicznego eksperta odbywać się będzie na podstawie podpisanych   
    bez zastrzeżeń, przez Zamawiającego, Protokołów odbioru asysty technicznej eksperta.
11. Zamawiając wymaga realizacji zlecenia asysty technicznej we wskazanym przez Zamawiającego miejscu na terenie Warszawy.
12. Świadczenie usługi asysty technicznej eksperta jest uprawnieniem Zamawiającego. Niewykorzystanie wszystkich przewidzianych w Umowie roboczogodzin nie rodzi po stronie Wykonawcy żadnych roszczeń w stosunku do Zamawiającego.
13. Wykonawca przeprowadzi szkolenia powdrożeniowe dla 4 osób, w turach po 2 osoby, z każdego zakresu wymienionego poniżej (łącznie 4 szkolenia – 2 z zakresu 1 i 2 z zakresu 2):

Zakres 1:

a) wdrożenie „Systemu Ochrony Poczty” w typowym środowisku korporacyjnym wykorzystując najlepsze praktyki podczas instalacji, konfiguracji i administracji systemem

b) zarządzanie, monitorowanie i rozwiązywanie problemów z przesyłaniem wiadomości pocztą elektroniczną przez „System Ochrony Poczty”

c) konfiguracja polityki dostępu w celu wyeliminowania zagrożeń związanych z wykorzystaniem poczty elektronicznej

d) tworzenie filtrów w celu egzekwowania polityki korporacyjnej dotyczącej wykorzystania poczty elektronicznej w celu zabezpieczenia poufnych informacji

e) konfiguracja „Systemu Ochrony Poczty” w celu wykrywania i zabezpieczania przed niechcianymi wiadomościami i wirusami

f) zarządzanie kwarantanną dla użytkowników poczty elektronicznej

g) tworzenie i zarządzanie raportami dotyczącymi bezpieczeństwa i wykorzystania poczty elektronicznej w korporacji

h) uwierzytelnianie użytkowników poczty elektronicznej

Zakres 2:

a) Szczegółowe informacje na temat "Systemu Ochrony komunikacji WWW"

b) Instalacja i implementacja "Systemu Ochrony komunikacji WWW" w różnych scenariuszach wdrażania

c) Instalacja usługi proxy "Systemu Ochrony komunikacji WWW"

d) Konfiguracja polis bezpieczeństwa "Systemu Ochrony komunikacji WWW"

e) Polityka dostępu do Internetu

f) Szyfrowanie i deszyfrowanie

g) Routing

h) Dostęp użytkowników

i) Filtrowanie URL

j) Definiowanie kategorii

k) Konfiguracja kategorii

l) Czasowe polityki dostępu

m) Reputacja sieci Web i jej używanie w polityce dostępu

n) Skanowanie zawartości z wykorzystaniem silników anti-malware

o) Inspekcja protokołu HTTPS

p) Metody uwierzytelniania "Systemu Ochrony komunikacji WWW"

q) Uwierzytelnianie użytkowników

r) Obrona przed złośliwym oprogramowaniem

s) Konfigurowanie funkcji zabezpieczeń danych

t) Administracja systemem raz rozwiązywanie problemów dotyczących "Systemu Ochrony komunikacji WWW"

Łączny czas trwania szkoleń z zakresu 1 i 2: minimum 48 godzin (zegarowych).

1. Wykonawca zobowiązany jest do przeprowadzenia szkoleń w ośrodku szkoleniowym na terenie Warszawy, w terminie do 24 miesięcy od daty podpisania bez zastrzeżeń protokołu odbioru   
   w zakresie dostawy systemu będącego przedmiotem niniejszego zamówienia.
2. Każdy uczestnik szkolenia otrzyma certyfikat jego ukończenia.
3. Szkolenia muszą być prowadzone w języku polskim.
4. Wykonawca musi dysponować odpowiednio wykwalifikowaną kadrą, której powierzy realizację przedmiotu zamówienia w zakresie szkoleń. Wymagane jest, aby trenerzy posiadali udokumentowane co najmniej 2-letnie doświadczenie w przedmiocie szkolenia z zakresu oferowanego rozwiązania.
5. Wykonawca powinien dysponować lub zapewnić na cele realizacji przedmiotu zamówienia bazą 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.
6. Wykonawca w terminie do 30 dni, od dnia podpisania bez zastrzeżeń protokołu odbioru   
   w zakresie dostawy systemu będącego przedmiotem niniejszego zamówienia, przedstawi Zamawiającemu do akceptacji Program szkolenia. Program 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.
7. Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy szkoleń – z rozpisaniem na dni i godziny i dostarczy je do 30 dni od dnia podpisania bez zastrzeżeń protokołu odbioru w zakresie dostawy systemu będącego przedmiotem niniejszego zamówienia. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu.
8. 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 i program szkolenia powinny zostać wydrukowane i rozdane uczestnikom szkolenia na pierwszym spotkaniu.
9. Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika do danego rodzaju szkolenia, pozwalające na samodzielną edukację z zakresu tematyki szkoleń (opracowania, wydruku materiałów szkoleniowych).
10. 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.

1. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć.
2. Koszty opracowania, transportu i powielenia materiałów ponosi Wykonawca.
3. 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:
4. 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.
5. 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 zegarowych szkolenia.

1. Koszty posiłków, dowozu, sprzętu i obsługi ponosi Wykonawca.
2. Potwierdzeniem prawidłowej realizacji szkoleń będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru szkoleń wraz z dołączonymi załącznikami tj. oryginalną listą obecności, harmonogramem i programem szkolenia oraz ankiety oceny warsztatu przeprowadzonej wśród uczestników warsztatu.