

Rawa Mazowiecka, 19.03.2025 r.

ZAPYTANIE OFERTOWE

Dotyczy projektu pn. Dostawa sprzętu i oprogramowania w ramach projektu „Cyberbezpieczny samorząd” w Urzędzie Miasta Rawa Mazowiecka w ramach: Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (DERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2 – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd”

I. ZAMAWIAJĄCY : Gmina Miasto Rawa Mazowiecka**II. OPIS PRZEDMIOTU ZAMÓWIENIA**

Miasto Rawa Mazowiecka występuje z zapytaniem ofertowym dotyczącym dostawy sprzętu komputerowego, oprogramowania oraz usług związanych z wdrożeniem systemów teleinformatycznych.

Przedmiot zamówienia:

Przedmiotem zamówienia jest dostawa UTM, oprogramowania przeciwdziałającemu wyciekowi danych oraz wdrożenie systemów teleinformatycznych.

Poniżej przedstawiono wymagania przedmiotów zamówienia:

CZĘŚĆ I

1. UTM – 1 sztuka

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

- 2 x GE RJ45 MGMT/DMZ Ports
- 2 x GE RJ45 WAN Ports
- 2 x GE RJ45 HA Ports
- 12 x GE RJ45 Ports
- 2 x 10 GE SFP+
- 4 x GE SFP Slots
- 4 x GE RJ45/ SFP

2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
 - Amazon Web Services (AWS).
 - Microsoft Azure.
 - Cisco ACI.
 - Google Cloud Platform (GCP).
 - OpenStack.
 - VMware NSX.
 - Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
 - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
 - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
 - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
 - Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).

7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).

7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimalny do 30.06.2026 roku.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

CZĘŚĆ II

1. Oprogramowanie przeciwdziałające wyciekowi danych – 70 licencji

Oprogramowanie przeciwdziałające wyciekowi danych

Oprogramowanie na licencji wieczystej z dwu letnim wsparciem na minimum 70 stanowisk.

1. Pełne wsparcie dla stacji roboczych z systemami Windows 7/Windows 8.1/Windows 10/Windows 11.
2. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2012 i nowszych.
3. Pomoc w programie (help) i dokumentacja do programu dostępna w języku angielskim.
4. Konsola administracyjna oraz komunikaty klienta muszą być w języku polskim.
5. Serwer administracyjny musi wspierać instalację w oparciu o bazę MS SQL.
6. Serwer administracyjny musi działać w architekturze serwer-klient, gdzie komunikacja serwera zarządzającego z klientem odbywa się przy pomocy agenta.
7. Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
8. Serwer administracyjny musi umożliwiać wykonanie instalacji/deinstalacji zdalnej klienta na stacjach roboczych.
9. Reguły DLP muszą być egzekwowane również w przypadku braku połączenia między klientem, a serwerem zarządzającym.
10. W przypadku braku połączenia klienta z serwerem zarządzającym, klient musi mieć możliwość lokalnego przechowywania informacji oraz zebranych danych do czasu ponownego połączenia z serwerem administracyjnym.

11. Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsol.
12. Administrator musi posiadać możliwość zarządzania bazą danych poprzez określone zadania:

kopia bazy danych, kopia oraz wyczyszczenie bazy danych, wyczyszczenie bazy danych. Administrator musi posiadać możliwość określenia wykonywania czasu związanego z wykonywaniem zadań na bazie danych. Zadania powinny być wykonywane co najmniej z interwałem: raz na tydzień, raz na dwa tygodnie, raz w miesiącu, raz na trzy miesiące.

13. Administrator musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych. Jeżeli rozmiar bazy danych osiągnie skonfigurowany rozmiar, najstarsze informacje muszą być usunięte z bazy danych, w celu nie przekroczenia skonfigurowanego rozmiaru bazy.

14. Serwer administracyjny programu musi mieć możliwość automatycznego pobierania aktualizacji

definicji kategoryzowania stron internetowych, aplikacji oraz rozszerzeń plików. Musi być możliwość wyłączenia automatycznego pobierania.

15. Administrator musi mieć możliwość tworzenia nowych kont administratorów w konsoli programu

jak i ich usuwania oraz klonowania.

16. Administrator musi mieć możliwość przypisywania jak i odbierania uprawnień do wybranych modułów programu. Uprawnienia muszą być podzielone na:

- a. Ustawienia, które określają możliwość wykonania konfiguracji na poszczególnym module,
- b. Logi, które określają możliwość wyświetlenia logów poszczególnego modułu.

17. Serwer musi posiadać możliwość synchronizacji użytkowników oraz stacji roboczych z domeną

Active Directory.

18. System musi posiadać możliwość logowania zdarzeń aktywności stacji roboczej, w oparciu o co najmniej:

- a. logowanie oraz wylogowanie użytkownika,
- b. włączenie oraz wyłączenie stacji roboczej,
- c. blokada oraz odblokowanie stacji roboczej,
- d. przejście w stan bezczynności stacji roboczej.

19. Administrator musi mieć możliwość, wymuszenia synchronizacji ustawień oraz logów, pomiędzy stacją roboczą, a serwerem, w czasie rzeczywistym.

20. Serwer administracyjny musi mieć możliwość ustawienia powiadomień dla użytkownika

końcowego, w przypadku złamania reguł ustawionych w modułach związanymi z ochroną DLP. W powiadomieniu administrator musi posiadać możliwość określenia własnej grafiki, kontaktowego adresu e-mail oraz odnośnika do polityki bezpieczeństwa organizacji.

21. Oprogramowanie musi posiadać możliwości audytu stacji roboczych/użytkowników w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, ruch sieciowy, wysyłane oraz odebrane wiadomości e-mail oraz wykonane czynności na plikach.

22. Administrator musi posiadać możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji oraz typów plików.

23. Administrator musi posiadać możliwość filtrowania oraz sortowania zebranych danych. Tak odfiltrowane dane, administrator może zapisać w postaci plików PDF bądź XLS.

24. Konsola musi posiadać możliwość wysyłania powiadomień, jeśli dany użytkownik przekroczy określoną dopuszczalną ilość wysyłanych maili oraz w przypadku przekroczenia dopuszczalnej ilości wysyłanych danych do sieci w danym dniu lub tygodniu.

25. Serwer musi posiadać możliwość wystania alertów, co najmniej za pośrednictwem wiadomości

email.

26. Serwer administracyjny musi posiadać możliwość konfiguracji raportów w oparciu o uruchomione aplikacje, podłączane urządzenia, odwiedzane strony internetowe, drukowane dokumenty, ruch sieciowy, wysyłane wiadomości e-mail oraz wykonywane czynności na plikach.

27. Raporty muszą być generowane w oparciu o wskazane stacje robocze, użytkowników bądź grupy w określonym przedziale czasu.

28. Raporty muszą być generowane do pliku PDF i/lub XLS, po podaniu lokalizacji zapisywanego pliku

lub na wskazany adres(y) e-mail.

29. Serwer administracyjny musi posiadać wbudowany serwer SMTP udostępniony przez producenta

oprogramowania.

30. Serwer administracyjny musi umożliwiać kategoryzację (tagowanie) plików na poziomie systemu plików lub na poziomie metadanych pliku.

31. Serwer administracyjny musi umożliwiać wykonanie zadania kategoryzacji (tagowania) plików, które już znajdują się na stacjach roboczych i zasobach sieciowych, ale również nowych plików, które powstaną na bazie już skategoryzowanych (otagowanych) plików.

32. Serwer administracyjny musi mieć możliwość kategoryzacji (tagowania) plików wrażliwych w oparciu o:

- a. aplikacje, z której zostały utworzone,
- b. lokalizację,
- c. adres URL,
- d. format pliku,
- e. zawartość pliku.

33. Administrator musi mieć możliwość wyszukiwania danych osobowych na zasobach zarówno

lokalnych jak i sieciowych.

34. Dla plików skategoryzowanych (otagowanych), musi być możliwe utworzenie następujących reguł:

- a. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików, do lokalizacji na określonych dyskach lokalnych,
 - b. blokowanie oraz zezwalanie na zapisywanie, przenoszenie do lokalizacji na dyskach zewnętrznych z możliwością określenia białej oraz czarnej listy tych urządzeń,
 - c. blokowanie oraz zezwalanie na drukowanie na określonych drukarkach,
 - d. blokowanie oraz zezwalanie na zapisywanie i przenoszenie do lokalizacji sieciowej,
 - e. blokowanie oraz zezwalanie na wysyłanie za pośrednictwem klientów pocztowych z możliwością określenia białej i czarnej listy adresów i domen,
 - f. blokowanie oraz zezwalanie na wysyłanie do poczty webowej,
 - g. blokowanie oraz zezwalanie na zapisywanie, przenoszenie plików do chmury,
- zarówno

za pomocą przeglądarki internetowej jak i aplikacji, w oparciu o co najmniej poniższe usługi:

- Dropbox,
- Google Drive,
- SharePoint,

- OneDrive Business,
 - OneDrive Personal.
 - h. blokowanie oraz zezwalanie na przesyłanie za pomocą komunikatorów,
 - i. blokowanie oraz zezwalanie na zapisywanie i przenoszenie danych poprzez usługę pulpitu
 - zdalnego,
 - j. blokowanie oraz zezwalanie na wykonywanie zrzutów ekranowych, skopiowania zawartości
 - oraz wirtualnego drukowania,
 - k. uruchomienie wybranego formatu pliku przez wskazaną przez administratora aplikację,
35. Serwer administracyjny musi umożliwiać możliwość zabezpieczenia korzystania z niezaufanych repozytoriów GIT.
36. Każda z polityk musi posiadać możliwość ustawienia jej w trybie powiadomienia dla użytkownika.
37. Serwer administracyjny musi dawać możliwość klasyfikacji pliku (tagowania) użytkownikowi na stacji roboczej. Klasyfikacja musi odbywać się poprzez integrację z menu kontekstowym.
38. Klasyfikacja użytkownika musi posiadać opcję, która uniemożliwi użytkownikowi zmianę klasyfikacji na niższą.
39. Serwer administracyjny musi umożliwiać określenie białych i czarnych list zawierających urządzenia pamięci masowej, drukarki fizycznych i sieciowych, lokalizacji sieciowych, adresów e-mail oraz domen, urządzeń przenośnych, firewire oraz bluetooth, które mogą być wykorzystywane do określenia reguł dostępu.
40. Serwer administracyjny musi posiadać funkcjonalność globalnego zablokowania lub zezwolenia na korzystanie z określonych folderów lokalnych, sieciowych, dysków o określonych literach oraz folderów synchronizacji z usługami chmury.
41. Serwer musi posiadać funkcjonalność skonfigurowania reguł dostępu dla urządzeń podłączanych do portu USB, urządzeń przenośnych, nośników optycznych CD/DVD, urządzeń Firewire, urządzeń podczerwieni, urządzeń Bluetooth, portów COM oraz LPT.
42. Serwer administracyjny musi posiadać możliwość zaszyfrowania całej powierzchni dysku w oparciu o funkcjonalność BitLocker z użyciem hasła lub modułu TPM.
43. Serwer administracyjny musi posiadać możliwość szyfrowania dysków zewnętrznych w oparciu o funkcjonalność BitLocker. Szyfrowanie oraz autoryzacja dla zaszyfrowanych nośników wymiennych musi być w pełni niezauważalna dla użytkownika.
44. Serwer administracyjny musi posiadać możliwość wyświetlenia i eksportu klucza odzyskiwania do zaszyfrowanych dysków oraz dysków wymiennych.
45. Serwer administracyjny musi posiadać możliwość wyszukiwania i ochrony plików w oparciu o ich zawartość, co najmniej o:
- a. numery kart kredytowych,
 - b. numer PESEL,
 - c. numer polskiego dowodu osobistego,
 - d. polski numer paszportu,
 - e. wyrażenia regularne,
 - f. określone ciągi znaków,

- g. numer IBAN.
46. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
47. Weryfikacja zawartości pliku w czasie rzeczywistym musi posiadać funkcjonalność OCR (Optical Character Recognition).
48. System musi posiadać możliwość importu własnych słowników do wyszukiwania danych.
49. W przypadku incydentu bezpieczeństwa, system musi wykonać duplikat pliku lub wiadomości e-mail, w którym znajdują się dane wrażliwe (tzw. funkcjonalność „Shadow-copy”).
50. Serwer administracyjny musi posiadać możliwość wyznaczenia progu ilości wystąpień danych wrażliwych, od jakich zostanie uruchomione zadanie klasyfikacji (tagowania).
51. Serwer administracyjny musi posiadać możliwość integracji klasyfikacji danych, z modulem DLP dostępnym na rozwiązaniu FortiGate.
52. Serwer administracyjny musi umożliwiać eksport logów do rozwiązania FortiSIEM.
53. Serwer administracyjny musi umożliwiać eksport identyfikatorów oznaczonych plików do rozwiązania FortiMail, które będzie w stanie kontrolować przesyłanie tak oznaczonych plików.
54. Serwer administracyjny musi umożliwiać integrację z Office365. Integracja musi pozwalać na:
- a. audyt i logowanie wiadomości e-mail,
 - b. audyt i logowanie operacji na plikach,
 - c. wprowadzanie polityk zabezpieczeń do wiadomości e-mail.
55. System musi umożliwiać integrację z narzędziami analitycznymi tj. Power BI, Tableau).
56. Serwer administracyjny musi posiadać konsolę dostępną z poziomu przeglądarki internetowej, służącą do raportowania i zarządzania stacjami roboczymi i urządzeniami mobilnymi.
57. Konsola musi wyświetlać informacje na temat bezpieczeństwa danych, produktywności pracowników oraz użycia sprzętu które są podzielone na:
- a. Bezpieczeństwo danych:
 - Przegląd informacji o incydentach bezpieczeństwa.
 - Przegląd danych przychodzących.
 - Przegląd danych wychodzących.
 - Przegląd informacji z Office365 które dotyczą m.in. pobierania, współdzielenia oraz lokalnego dostępu do plików.
 - Podłączane/odłączane urządzenia przenośne.
 - b. Produktywność:
 - Przegląd informacji na temat produktywności użytkowników.
 - Aktywność użytkowników podczas przeglądania stron WWW oraz korzystania z aplikacji.
 - Trendy.
 - c. Eksploatacja sprzętu:
 - Przegląd informacji na temat eksploatacji sprzętu komputerowego.
 - Eksploatacja sprzętu komputerowego, najbardziej nieaktywne komputery.
 - Eksploatacja drukarek.
 - Eksploatacji sieci.
58. Konsola webowa musi posiadać możliwość konfiguracji/zmiany domyślnego serwera SMTP.

59. Konsola webowa musi umożliwiać weryfikację wersji zainstalowanego oprogramowania klienta wraz z możliwością aktualizacji do nowej wersji lub dezaktywacji tego oprogramowania.

60. Konsola webowa musi umożliwiać wygenerowanie raportu w postaci pliku DOCX, który zawiera informacje nt:

- plików przenoszonych na nośniki USB i inne urządzenia przenośne,
- plików przesłanych za pomocą wiadomości e-mail,
- plików przesłanych za pomocą poczty webowej,
- plików przesłanych do Internetu,
- plików wysłanych za pomocą komunikatorów,
- plików przesłanych na dyski chmurowe,
- analiza sposobu korzystania z aplikacji,
- analiza korzystania z Internetu,
- analiza wykorzystania porali do poszukiwania pracy.

2. Wdrożenie systemów teleinformatycznych – 1 sztuka

Usługi wdrożeniowe oprogramowania przeciwdziałającego wyciekowi danych (DLP), którego głównym celem jest zabezpieczenie przed utratą lub nieautoryzowanym dostępem do informacji poufnych. Oprogramowanie to ma zostać zainstalowane na serwerze działającym pod kontrolą systemu Windows Server co najmniej w wersji 2016 oraz powinno być obsługiwane za pomocą dwóch konsol: aplikacyjnej i webowej, w celu ułatwienia zarządzania systemem.

- Wykonawca przeprowadzi analizę wymagań Zamawiającego, zaczynając od zebrania wymagań od różnych zespołów w organizacji, aby określić, jakie funkcje i moduły oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych będą najbardziej przydatne.
- Wykonawca przeprowadzi planowanie wdrożenia w oparciu o przeprowadzoną analizę, uwzględniając harmonogram, zasoby, zadania.
- Wykonawca przygotuje środowisko wirtualne, upewniając się, że wszystkie wymagania stawiane przez oprogramowanie zostały spełnione, włączając w to odpowiednie zasoby, konfigurację systemu operacyjnego oraz konfigurację sieciową niezbędną do prawidłowego działania oprogramowania.
- Wykonawca wykona konfigurację baz danych niezbędnych do wdrożenia oprogramowania, włączając to prawidłowe połączenie pomiędzy oprogramowaniem a bazą danych.
- Wykonawca zainstaluje oprogramowanie przeciwdziałającego wyciekowi danych.
- Wykonawca wykona integrację z istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz przygotuje konta usługi oprogramowania, włączając w to konfigurację uprawnień dla konta usługi. Wykonawca przeprowadzi testy wykonanej integracji w celu upewnienia się, że informacje są poprawnie synchronizowane między oprogramowaniem a istniejącymi systemami w środowisku Zamawiającego, w tym z kontrolerem domeny oraz czy synchronizacja użytkowników, grup i innych obiektów z kontrolera domeny do oprogramowania działa w sposób prawidłowy. Wykonawca będzie monitorował i utrzymywał integrację między oprogramowaniem przez cały okres trwania wdrożenia.
- Wykonawca uruchomieni i skonfiguruje konsolę zarządzającą, wprowadzi klucz dostępowy i usunie dane demonstracyjne.
- Wykonawca przeprowadzi instruktaż w zakresie prawidłowej instalacji agentów niezbędnych do prawidłowego działania oprogramowania, uwzględniając utworzenie odpowiednich grup i polityk wdrożeniowych dla agentów. Po zakończonej instalacji agentów, Wykonawca przeprowadzi testy poprawności instalacji i komunikacji agentów z serwerem oprogramowania.
- Wykonawca przeprowadzi testy instalacji w celu upewnienia się, że instalacja oprogramowania przebiegła bez problemów i wszystkie komponenty zostały poprawnie zainstalowane na serwerze oraz urządzeniach końcowych.

J. Wykonawca wykona konfigurację kategorii danych i danych wrażliwych oraz zdefiniuje wykrywanie kategorii:

- Numery kart kredytowych
- Numery IBAN
- Numery dowodów osobistych
- Polski numer paszportu
- Numer PESEL

K. Wykonawca skonfiguruje alerty związane z usługami oraz zabezpieczeniem DLP oraz przetestuje poprawność ich działania na danych testowych.

L. Wykonawca skonfiguruje zadania archiwizacji danych oraz usuwania starych wpisów z bazy danych.

M. Wykonawca przetestuje działanie polityk i wprowadzi ich aktualizację w przypadku wykrycia braku ich skutecznego działania.

N. Wykonawca wygeneruje z prawidłowo wdrożonego oprogramowania raport audytu bezpieczeństwa i przeprowadzi analizę aktywności użytkowników oraz przepływu informacji w organizacji.

O. Wykonawca przeprowadzi testy monitorowania i raportowania, weryfikując czy raporty generowane przez oprogramowanie zawierają poprawne i aktualne informacje.

P. Wykonawca przeprowadzi testy wydajnościowe w celu upewnienia się, że infrastruktura oprogramowania działa płynnie i efektywnie, nawet przy dużej liczbie urządzeń i użytkowników.

Q. Wykonawca przeprowadzi testy przywracania awaryjnego, włączając w to procedury przywracania awaryjnego w celu upewnienia się, że w razie konieczności można szybko przywrócić działanie systemu oprogramowania sieciowych po awarii.

III Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV)

CPV 72268000-1

CPV 48000000-8

CPV 72263000-6

IV. TERMIN REALIZACJI UMOWY

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Dostawy sprzętu oraz z części I będą realizowane w ciągu 21 dni. Usługi i Dostawy oprogramowania wdrożenia z części II będą realizowane w ciągu 120 dni.

Przedmiot umowy będzie dostarczany przez Wykonawcę do miejsc wskazanych przez Zamawiającego w zakresie dostawy sprzętu.

Terminy realizacji zamówienia mogą ulec zmianie, w zależności od wystąpienia okoliczności, których nie można było przewidzieć w dniu zawarcia umowy lub w sytuacjach nieprzewidzianych lub uzasadnionych, za zgodą obu stron.

V Warunki udziału w postępowaniu

1. udzielenie zamówienia mogą się ubiegać wykonawcy, którzy:
 - nie podlegają wykluczeniu na podstawie ustawy prawo zamówień publicznych,

- spełniają warunki udziału w postępowaniu w zakresie kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile obowiązek ich posiadania wynika z odrębnych przepisów. Zamawiający nie określa szczegółowo ww. warunku.
 - spełniają warunki udziału w postępowaniu w zakresie sytuacji ekonomicznej lub finansowej. Zamawiający nie określa szczegółowo ww. warunku.
 - spełniają warunki udziału w postępowaniu w zakresie zdolności technicznej lub zawodowej.
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
 3. Na potwierdzenie spełnienia warunku udziału w postępowaniu, dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca wykazał się odpowiednim doświadczeniem, tj. w ciągu ostatnich 3 lat przed upływem terminu składania ofert, w tym okresie realizuje, bądź zrealizował należycie co najmniej dwie usługi w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 100 000 złotych brutto.
 4. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
 5. Wykonawca, który polega na zdolnościach innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

VI Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem wag tych kryteriów i sposobu oceny ofert

Do części I zamówienia:

1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	90
2.	Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę	10

2. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.
3. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.
4. Przy ocenie ofert w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:
 - Cena – znaczenie 90% (maksymalnie do 90 pkt)
 - Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
 - Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

$$C = CC_{\min} / CC_{\text{of}} \times 90$$

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

- Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.

5. Kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę” stanowi 10 możliwych do uzyskania punktów.

6. Sumaryczna liczba punktów zostanie obliczona według wzoru:

$$W = C + E$$

gdzie:

W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

C – liczba punktów przyznanych w kryterium „Cena”,

E – wartość punktowa kryterium „Przyjmowanie możliwości wykonania zamówienia poza godzinami 8.00-17.00 tj. przez całą dobę”,

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku

7. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

8. W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie kryterium ceny jako kryterium o wadze przekraczającej 60%, ze względu na określenie w opisie przedmiotu zamówienia wymagań jakościowych odnoszących się do co najmniej głównych elementów składających się na przedmiot zamówienia.

Do części II zamówienia:

9. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami:

Lp.	Nazwa kryterium	Waga (pkt)
1.	Cena (całkowity koszt wykonania zamówienia)	70
2.	Termin realizacji	30

10. Przy wyborze oferty Zamawiający będzie stosować zasadę, że oferta nieodrzucona, zawierająca najwyższą liczbę punktów przyznanych według powyższych kryteriów, jest ofertą najkorzystniejszą.

11. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień treści złożonych przez nich ofert.

12. Przy ocenie ofert w kryterium „Cena” (C) punkty zostaną przyznane w poniższy sposób:

- Cena – znaczenie 70% (maksymalnie do 70 pkt)
- Kryterium ceny będzie rozpatrywane na podstawie ceny brutto podanej przez Wykonawcę w Formularzu Ofertowym.
- Punkty w kryterium „Cena” będą obliczane na podstawie wzoru:

$$C = CC \text{ min} / CC \text{ of} \times 70$$

gdzie:

C – punkty przyznane Wykonawcy w ramach kryterium „Cena”

CC min – najniższa cena brutto spośród badanych ofert

CC of – cena brutto badanej ofert

- Do wzoru zostaną przyjęte ceny podane przez Wykonawców w Formularzu Oferty stanowiącym Załącznik nr 1 do SWZ.

13. Kryterium „Termin realizacji” stanowi maksymalnie do 30 pkt przy kryteriach:

- Powyżej 120 dni – 0 pkt;
- Do 100 dni – 10 pkt;
- Do 80 dni – 20 pkt;
- Do 60 dni – 30 pkt.

14. Sumaryczna liczba punktów zostanie obliczona według wzoru:

$$W = C + E$$

gdzie:

W – łączna liczba punktów przyznanych w poszczególnych kryteriach,

C – liczba punktów przyznanych w kryterium „Cena”,

E – wartość punktowa kryterium „Termin realizacji”,

Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku

15. Wszystkie obliczenia dokonywane będą z dokładnością do dwóch miejsc po przecinku.

16. W związku z zaistnieniem przesłanki o której mowa w art. 246 ust. 2 PZP możliwe było zastosowanie kryterium ceny jako kryterium o wadze przekraczającej 60%, ze względu na określenie w opisie przedmiotu zamówienia wymagań jakościowych odnoszących się do co najmniej głównych elementów składających się na przedmiot zamówienia.

VII Wykaz oświadczeń lub dokumentów, jakie mają złożyć wykonawcy w celu wykazania spełniania warunków udziału w postępowaniu oraz niepodlegania wykluczeniu z postępowania

1. Wykaz dostaw wykonanych w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - tj. w tym okresie, wraz z podaniem ich wartości, dat wykonania i podmiotów na rzecz, których usługi zostały wykonane, przed upływem terminu składania ofert, w co najmniej dwóch usług w zakresie dostawy sprzętu komputerowego na kwotę co najmniej 100 000 złotych brutto wraz z dowodem należytego ich wykonania.
2. Wykonawca jest zobowiązany do wypełnienia obowiązku informacyjnego przewidzianego w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskał (w przypadku korzystania z podwykonawców/ podmiotów trzecich/wykonawców wchodzących w skład konsorcjum) w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

VIII. ZGŁASZANIE PYTAŃ I WĄTPLIWOŚCI

Wszelkie pytania i wątpliwości dotyczące prowadzonego postępowania należy kierować poprzez portal <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl/>.

Oferenci mogą zadawać pytania do przedmiotu zamówienia najpóźniej 2 dni robocze przed zakończeniem terminu składania ofert.

Jeżeli wniosek o wyjaśnienie treści zapytania ofertowego wpłynie po upływie terminu, o którym mowa powyżej lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.

Odpowiedzi będą udzielane za pośrednictwem portalu <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl> w ciągu 2 dni roboczych.

W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść zapytania ofertowego.

Zapytanie ofertowe wraz ze zmianami upublicznione zostanie w Bazie Konkurencyjności.

IX. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca pozostaje związany złożoną ofertą przez okres 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z zakończeniem terminu składania ofert.

X. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

- a) Do oferty winny być dołączone wszystkie dokumenty i oświadczenia wskazane w zapytaniu ofertowym.
- b) Oferta oraz załączniki do oferty muszą być sporządzone w języku polskim.
- c) W przypadku składania Oferty w siedzibie Zamawiającego (osobiście lub pocztą/kurierem) należy złożyć Ofertę wraz z załącznikami w formie pisemnej, na papierze, z podpisami i pieczęciami w wyznaczonych miejscach (podpisy muszą być złożone przez Oferenta w taki sposób, aby możliwe było odczytanie podpisu (podpis może być uzupełniony pieczętką). Każda poprawka w ofercie musi być podpisana i opatrzona datą przez składającego Ofertę. Oświadczenia mają być złożone w oryginale. Kopie wymaganych dokumentów winny być poświadczone „za zgodność z oryginałem” przez składającego ofertę, z datą poświadczenia.
- d) W przypadku składania ofert przez Bazę Konkurencyjności dopuszcza się:
 - złożenie oferty wraz z załącznikami podpisanymi kwalifikowanym podpisem elektronicznym lub
 - złożenie oferty wraz z załącznikami podpisanymi elektronicznym podpisem zaufanym.
- e) Wszelkie koszty związane z przygotowaniem oferty i inne koszty ponosi Oferent.

XI. MIEJSCE I TERMIN SKŁADANIA OFERT

Ofertę należy złożyć poprzez portal <https://bazakonkurencyjnosci.funduszeuropejskie.gov.pl>, do dnia **27 marca 2025 roku**.

Otwarcie złożonych ofert nastąpi niezwłocznie po wyznaczonym terminie ich składania w siedzibie Zamawiającego.

XII. WYTYCZNE ODNOŚNIE CENY PRZEDSTAWIONEJ W OFERCIE

1. Cena musi uwzględniać wszystkie wymagania zapytania ofertowego oraz obejmować wszelkie koszty jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.
2. Cena musi być wyrażona w polskich złotych, liczbowo, z dokładnością do dwóch miejsc po przecinku. Oferta musi zawierać należny podatek VAT. Prawidłowe ustalenie stawki należnego podatku VAT należy do obowiązków Wykonawcy, zgodnie z przepisami ustawy o podatku od towarów i usług oraz o podatku akcyzowym.

INFORMACJE DOTYCZĄCE WALUTY ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Rozliczenia między Zamawiającym a Wykonawcą dokonywane będą w walucie polskiej, w złotych (PLN).

XIII. OCENA OFERT POD WZGLĘDEM FORMALNYM I DOPUSZCZENIE DO OCENY PUNKTOWEJ

1. Zamawiający dokona oceny ofert pod względem formalnym oraz zgodności z niniejszym zapytaniem ofertowym.
2. Oferta zostanie odrzucona, jeśli:
 - a) została złożona po wyznaczonym terminie;
 - b) została złożona w niewłaściwym miejscu;
 - c) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
 - d) do oferty nie załączono wszystkich wymaganych dokumentów przewidzianych w Zapytaniu ofertowym;
 - e) zaoferowana cena przez danego Wykonawcę przewyższa kwotę, którą Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia.
 - f) jest niezgodna z wymaganiami określonymi w Zapytaniu ofertowym;
 - g) jest niezgodna z obowiązującymi przepisami prawa;
 - h) jest niekompletna lub nie będzie zawierała wszystkich wymaganych przez Zamawiającego dokumentów, oświadczeń, podpisów.
 - i) Oferent nie spełnia warunków udziału w postępowaniu;
3. Zamawiający może wezwać Oferentów, którzy w określonym terminie nie złożyli wymaganych przez Zamawiającego oświadczeń lub dokumentów, lub którzy nie złożyli pełnomocnictw, albo którzy złożyli wymagane przez Zamawiającego oświadczenia i dokumenty, zawierające błędy, omyłki pisarskie bądź rachunkowe, niespójności lub nie potwierdzające spełnienia przez Oferentów warunków udziału w postępowaniu lub którzy złożyli wadliwe pełnomocnictwa, do ich złożenia w wyznaczonym terminie, chyba, że mimo ich złożenia oferta podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.
4. Zamawiający może w toku badania i oceny ofert żądać od Oferentów wyjaśnień dotyczących treści złożonych ofert.
5. Z tytułu odrzucenia oferty Wykonawcom nie przysługują żadne roszczenia przeciw Zamawiającemu.
6. Żadne informacje dotyczące procesu oceny oraz wyboru ofert nie zostaną ujawnione Oferentom lub innym osobom, niezaangażowanym oficjalnie w proces oceny i wyboru oferty.

7. Zamawiający odrzuci ofertę Oferenta, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdzi, że oferta zawiera informacje nieprawdziwe lub niemożliwe do udokumentowania.
8. Zamawiający wymaga, aby ofertę wraz z załącznikami podpisała osoba uprawniona do reprezentowania Wykonawcy. Jeżeli upoważnienie nie wynika z dokumentów rejestrowych, Wykonawca zobowiązany jest dołączyć do oferty stosowne pełnomocnictwo.

XIV. FORMALNOŚCI JAKIE POWINNY ZOSTAĆ DOPEŁNIONE W CELU ZAWARCIA UMOWY

1. Zamawiający zastrzega prawo do unieważnienia postępowania bez podania przyczyny oraz do odrzucenia oferty, jeżeli zaoferowana cena przekroczy kwotę przeznaczoną na sfinansowanie całości zamówienia lub danej części zamówienia, w przypadku złożenia oferty częściowej.
2. O unieważnieniu postępowania ofertowego Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy:
 - a. ubiegali się o udzielenie zamówienia – w przypadku unieważnienia postępowania przed upływem terminu składania ofert;
 - b. złożyli oferty – w przypadku unieważnienia postępowania po upływie terminu składania ofert;
3. Zamawiający podpisze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę z punktu widzenia kryteriów przyjętych w zapytaniu ofertowym, chyba że Zamawiający unieważni postępowanie.
4. Niezwłocznie po wyborze najkorzystniejszej oferty, Zamawiający poinformuje o wynikach postępowania umieszczając informację na Bазie Konkurencyjności.
5. Wykonawca, którego oferta zostanie uznana za najkorzystniejszą, przed podpisaniem umowy zobowiązany jest do złożenia informacji o osobach umocowanych do zawarcia umowy i okazania ich pełnomocnictwa, jeżeli taka konieczność zaistnieje.
6. Termin i miejsce podpisania umowy:
 - a. Wykonawca, którego oferta została wybrana jest zobowiązany do zawarcia umowy z Zamawiającym w terminie i miejscu wskazanym przez Zamawiającego, lecz nie później niż w terminie 7 dni od wskazanego terminu pod rygorem nie zawarcia umowy. Odpowiednio stosuje się pkt poniżej;
 - b. jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert bez przeprowadzenia ich ponownego badania i oceny.

XV. Załączniki:

- Załącznik nr 1 – Formularz oferty
- Załącznik nr 2 – Oświadczenie dotyczące braku podstaw wykluczenia
- Załącznik nr 3 - Wykaz usług
- Załącznik nr 4 – Projekt umowy