Ministerstwo Rozwoju i Technologii **Warszawa, 05.03.2025 r.**

ul. Plac Trzech Krzyży 3/5

00-507 Warszawa

ZAPYTANIE O WYCENĘ DO OSZACOWANIA WARTOŚCI ZAMÓWIENIA

Ministerstwo planuje uruchomić postępowanie przetargowe o udzielenie zamówienia publicznego na dostawę serwerów wraz z oprogramowaniem oraz dostawę oprogramowania serwerowego i bazodanowego

Uprzejmie prosimy o wycenę, poniżej opisanych minimalnych wymagań stanowiących przedmiot planowanego do wszczęcia postępowania przetargowego.

Zamówienie zostanie podzielone na trzy części:

1. Część I, tj. dostawa serwerów wraz z oprogramowaniem;
2. Część II, tj. dostawa dostawę oprogramowania serwerowego i bazodanowego.

Zamawiający zamierza podzielić zamówienie na części. Tym samym Zamawiający dopuszcza składanie ofert częściowych, tj. Wykonawca może złożyć ofertę na jedną lub dwie części zamówienia.

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest Rozbudowa infrastruktury serwerowej.

Zamówienie podzielone jest na dwie części:

1. Część I, tj. dostawa serwerów wraz z oprogramowaniem,
2. Część II, tj. dostawa oprogramowania serwerowego i bazodanowego

Przedmiotem zamówienia w Części II jest dostawa oprogramowania serwerowego i bazodanowego, która zostanie zrealizowana zgodnie z poniższym wykazem:

Lp.	Numer katalogowy	Produkt	Rodzaj licencjonowania	Liczba produktów
1	6QK-00001	Azure prepayment	Subskrypcja	50
2	9EA-00271	Win Server DC Core ALng LSA 16L z Software Assurance	Licencja nieograniczona w czasie	6
3	9EA-00039	Win Server DC Core ALng LSA 2L z Software Assurance	Licencja nieograniczona w czasie	144

II. TERMIN REALIZACJI ZAMÓWIENIA

Dostawa oprogramowania i subskrypcji stanowiących przedmiot zamówienia zostanie zrealizowana w terminie **do …… dni** (**zgodnie z liczbą dni wskazaną w Formularzu Ofertowym**) od dnia zawarcia umowy.

W ww. terminie Wykonawca zobowiązany jest do dostarczenia:

1. oprogramowania serwerowego i bazodanowego;
2. przesłania drogą mailową na adres ..... zgłoszenia realizacji zamówienia oraz udostępnienia spersonalizowanej strony pozwalającej upoważnionym ze strony Zamawiającego osobom na:
   a) pobieranie oprogramowania i subskrypcji,
   b) pobieranie kluczy aktywacyjnych do oprogramowania i subskrypcji,
   c) sprawdzanie liczby zakupionych licencji i subskrypcji w wykazie oprogramowania.

III. MINIMALNE WYMAGANIA realizacji przedmiotu zamówienia

1. Oferowane Produkty muszą być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).
2. Zamawiający nie dopuszcza zaoferowania licencji/subskrypcji w modelu CSP.
3. Ogólne zasady zakupu licencji Producenta Produktów muszą być zgodne z postanowieniami umowy ramowej Microsoft Enterprise Master Agreement nr 80E60204 (EA);
4. Zamawiający posiada zawartą umowę Enterprise Agreemant, ważna do 30.06.2028 r.
5. Wraz z licencjami Wykonawca dostarczy klucze aktywacyjne (jeśli są wymagane), nośniki instalacyjne lub dostęp do źródła, z którego można pobrać pakiet instalacyjny, dokumenty lub informacje potwierdzające legalność dostarczonego oprogramowania.
6. Oprogramowanie i subskrypcje oprogramowania muszą gwarantować prawo instalacji najnowszej wersji oprogramowania dostępnej w trakcie trwania umowy, możliwość wykorzystania wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego, licencje muszą pozwalać na swobodne przenoszenie pomiędzy komputerami (np. w przypadku wymiany sprzętu);
7. Zamawiający dopuszcza oferowanie produktów o szerszej niż opisana funkcjonalności.
8. Zamawiający wymaga zagwarantowania niezmienności cen producenta oferowanych produktów lub jego spółek zależnych (Producenta) na produkty w całym okresie trwania umowy, z wyłączeniem zmian kursowych EUR/PLN.
9. Oprogramowanie musi pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami (np. w przypadku wymiany lub uszkodzenia sprzętu).
10. Oferowane subskrypcje usług hostowanych muszą zapewniać posiadanie powszechnie uznanych i rozpowszechnionych standardów i normatywów potwierdzonych aktualnymi wynikami niezależnych audytów, w szczególności:
    a) ISO/IEC 27001, 27002, 27017, 27018,
    b) ISO/IEC 20000-1,
    c) ISO/IEC 22301,
    d) SOC 1, SOC 2, SOC 3,
    e) CIS Benchmark.
    f) Open Authentication Standard – OAuth
11. Oferowane pakiety subskrypcji oprogramowania muszą zapewniać:
    a) Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),
    b) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach platformy,
    c) Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO,
    d) Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
    e) Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
    f) Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi,
    g) Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory,
    h) Dostępność mechanizmu uwierzytelnienia wieloskładnikowego,
    i) Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”,
    j) Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
    k) Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
    l) Wbudowane mechanizmy zabezpieczające przed atakami DDoS,

m) Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km,

n) Spełnienie wymagań w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych

o) Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego.

p) Zgodność z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO),

q) Przetwarzane/składowane w usłudze dane pozostają własnością Zamawiającego,

r) Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.

s) Gwarancję braku dostępu przez podmioty trzecie do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody Zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy.

12. Oprogramowanie musi pozwalać na udzielenie licencji oprogramowania dla jednostek stowarzyszonych.
13. Z uwagi na szeroki zakres funkcjonalny i terytorialny wdrożenia planowanego na bazie zamawianego oprogramowania oraz konieczności minimalizacji kosztów związanych z wdrożeniem, szkoleniami i eksploatacją systemów, Zamawiający wymaga produktów, umożliwiających wykorzystanie wspólnych i jednolitych procedur masowej instalacji, uaktualniania, zarządzania, monitorowania i wsparcia technicznego oraz jednolitych mechanizmów wykorzystania tożsamości cyfrowej.
14. Zamawiający wymaga zaoferowania licencjonowania gwarantowanego przez Producenta produktów, umożliwiającego w okresie trwania umowy instalację subskrypcji z zamawianego zakresu produktów z rozliczaniem rocznym.
15. Wykonawca zapewni dostęp do spersonalizowanej strony pozwalającej upoważnionym osobom ze strony Zamawiającego na:
    a) Pobieranie zakupionego oprogramowania,
    b) Aktywację zakupionego oprogramowania,
    c) Sprawdzanie liczby zakupionych produktów w wykazie zakupionych produktów.
16. Po dziewięćdziesięciu (90) dniach od zakończenia okresu trwania umowy Wykonawca zapewni możliwość wyłączenia konta Zamawiającego na spersonalizowanej stronie Producenta i usunięcie jego danych.
17. Wykonawca zapewni obronę Zamawiającego z tytułu roszczeń strony trzeciej za naruszenie przez oferowany produkt prawa autorskiego, w przypadku niezwłocznego powiadomienia Wykonawcy o roszczeniu odszkodowawczym.
18. Jeżeli nowa wersja produktu zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tego produktu przez Zamawiającego.
19. W przypadku, gdy dostarczone przez Wykonawcę produkty nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowodują zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu Oprogramowania.
20. Produkty dostarczone przez Wykonawcę nie mogą powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nimi oprogramowania.
21. produkty przekazane będą w najnowszej wersji dostępnej w chwili złożenia oferty, muszą być kompatybilne i współdziałać w sposób niezakłócony ze sprzętem i oprogramowaniem

funkcjonującym u Zamawiającego oraz nie mogą powodować zakłóceń pracy środowiska systemowo-programowego Zamawiającego.

22. Wszystkie elementy usług muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę katalogową.
23. Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
24. Możliwość dodawania własnych nazw domenowych do usługi katalogowej.
25. Dostępność portalu administracyjnego do zarządzania usługami oraz zasadami grup.
26. Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
27. W okresie obowiązywania subskrypcji usługi będą przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, w przypadku podjęcia decyzji o baraku jej kontynuacji, Usługi będą przechowywać dane Zamawiającego, które zostały w nich zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją zostanie wyłączone a dane Zamawiającego zostaną usunięte.
28. Dostęp do usług musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
29. Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w usługach własnością Zamawiającego.
30. Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
31. Usługi muszą spełniać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych, w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych.
32. Usługi muszą zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
33. Dostęp do portalu administracyjnego zapewniającego szczegółowe opcje konfiguracji usług, zarówno w portalu online, jak i za pośrednictwem zautomatyzowanego zarządzania przy użyciu poleceń programu PowerShell,
34. Dostarczone subskrypcje muszą uprawniać Zamawiającego do wykorzystywania aktualnych, obowiązujących wersji subskrypcji (prawo do wykonywania upgrade) oraz historycznie wydanych przez producenta oprogramowania, niższych wersji oprogramowania (prawo do wykonywania downgrade).
35. Narzędzie udostępniające przestrzeń dyskową dostępną z dowolnego miejsca i synchronizowaną z komputerem PC lub Mac użytkownika w celu zapewnienia dostępu w trybie offline (również mobilna).

IV. Opis wymaganych minimalnych funkcjonalności subskrypcji oprogramowania Azure prepayment

1. Pakiet subskrypcji standardowej, powszechnie dostępnej przez Internet usługi hostowanej typu COTS (Commercial Of-The-Shelf) udostępniający skalowalną platformę i pozwalający wykorzystać w ramach zakupionej puli zasobów – maszyny wirtualne, systemy operacyjne, silniki baz danych oraz inne aplikacje i usługi PaaS oraz IaaS spełniającą poniżej opisane wymagania.
2. W ramach dostarczonego pakietu subskrypcji Azure prepayment Zamawiający będzie miał prawo do pobierania zasobów w terminie od zawarcia umowy do 30.06.2028 r.
3. Pula zasobów zakupionych w pakiecie musi umożliwić wykorzystanie:
   a) Minimum 1 jednostki obliczeniowej o parametrach - 1 rdzeń procesora, 1,7 GB RAM, pod kontrolą systemu operacyjnego Windows Server lub Linux (wybrane dystrybucje),
   b) Minimum 50 GB dostępnej lokalnie redundantnej przestrzeni dyskowej,
   c) Minimum 50 GB dostępnej georedundantnej przestrzeni dyskowej (odległości min. 100km między lokalizacjami),
   d) Minimum 100 GB transferu danych do i z usługi miesięcznie.
4. Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług.
5. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów

zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
6. Możliwość wyboru różnych rodzajów dysków i ich pojemności.
7. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów, z możliwością zdalnego dostępu.
8. Komunikacja z mechanizmami zarządzania usługi poprzez REST API.
9. Możliwość przechowywania danych spełniająca następujące wymagania (opcjonalnie dostępnych w ramach usługi):
   a) Wysoka skalowalność, auto-partycjonowanie, load-balancing,
   b) Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka,
   c) Wsparcie dla systemów klienckich Windows i Linux,
   d) Skalowalność pojedynczego zasobu pamięci 500TB,
   e) Replikacja danych - min. 3 kopie w ramach pojedynczej lokalizacji,
   f) Replikacja do innej lokalizacji oddalonej o min 100km od lokalizacji podstawowej,
   g) Udostępnienie zasobów pamięci poprzez REST API,
   h) Gotowe biblioteki programistyczne środowisk programowania: .NET, Java/Android, Node.js, PHP, Ruby, Python, PowerShell.
10. Konfigurowalne usługi wyszukiwania treści w zasobach własnych i internet.
11. Konfigurowalne usługi analizy wyszukanych treści.
12. Dostępność usług umożliwiających uruchamianie aplikacji WWW w modelu gotowej do wykorzystania usługi, z utrzymywanymi przez producenta usług komponentami infrastruktury i możliwości w pełni automatycznego skalowania. Usługi te powinny zapewniać możliwość uruchamiania aplikacji działających w minimum następujących technologiach: ASP .NET, PHP, Python, Java, Node,js.
13. Dostępność gotowej usługi realizującej backup serwerów oraz stacji roboczych – zarówno wirtualnych, jak i fizycznych. Usługa musi zapewniać całościowy scenariusz backupu, bez konieczności instalacji komponentów spoza samej usługi, z możliwością definiowania polityk backupowych, wbudowanym szyfrowaniem i możliwością zdefiniowania rozporoszonej geograficznie przestrzeni magazynowej.
14. Dostępność relacyjnej i nierelacyjnej bazy danych, w tym oparte o technologię Hadoop, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
15. Dostępność środowisk zapewniających możliwość strumieniowego przetwarzania danych z użyciem klastrów opartych o technologie Apache Kafka i Apache Storm dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
16. Możliwość serializacji do określonego formatu tekstowego (np. opartego o XML lub JSON) rozwiązań opartych o maszyny wirtualne, wraz z ich konfiguracją, w sposób umożliwiający ich automatyczną deserializację i utworzenie na tej podstawie gotowego do pracy środowiska.
17. Dostępny portal administracyjny, pozwalający na uruchamianie usług poprzez wybór spośród dostępnych usług.
18. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
19. Włączenie reguł wymuszających stosowanie się do odpowiedniej nomenklatury nazewnictwa zasobów w obrębie środowiska, wymuszając wykorzystanie ustalonego modelu nazw, prefiksów dla określonych typów zasobów.
20. Dostępność usług umożliwiających utworzenie prywatnego repozytorium obrazów kontenerów w standardzie zgodnym z Docker.
21. Dostępność usług umożliwiających utworzenie gotowej do działania infrastruktury utrzymania aplikacji w formie kontenerów zgodnych z Docker – usługi działającej w formie PaaS, w szczególności bez konieczności ręcznego konfigurowania węzłów roboczych i zarządzających
22. Dostępność relacyjnych baz danych, zgodnych z MySQL i z PostgreSQL, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
23. Dostępność bazy danych typu NoSQL, oferującej API dostępowe zgodne z MongoDB dostępnej jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
24. Przynajmniej dwa jasno zdefiniowane poziomy spójności danych dla bazy NoSQL
25. Możliwość automatycznej dystrybucji danych pomiędzy różne regiony oraz ulokowane w nich centra obliczeniowe wraz z możliwością ręcznego jak i automatycznego przełączania replik
26. Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a usługodawcą usług chmurowych w technologii opartej o światłowody.
27. Posiadanie przez producenta centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.
28. Akcelerowana, definiowana programowo sieć wirtualna w środowisku, wspierająca akceleracje SR-IOV, realizowana na akcelerowanych interfejsach sieciowych FPGA, do 30Gb/s.
29. Możliwość śledzenia ruchu sieciowego
30. Dostępność mechanizmów analizy działania wielowarstwowych aplikacji poprzez umieszczanie kodu JavaScript wewnątrz stron internetowych lub doklejanie kodu do aplikacji czy instalacji agenta na serwerze umożliwiając korelowanie i analizowanie od frontu po sam serwer aplikacji

czy bazy danych

31. Możliwość wykorzystania usług SMB 3.0 do współdzielenia plików wykorzystując szyfrowanie podczas transmisji jako usługa.
32. Możliwość zdefiniowania szablonu maszyny wirtualnej włącznie z konfiguracją aplikacji, uruchamiania serwisów poprzez zdefiniowanie stanu oczekiwanego w postaci plików konfiguracyjnych.
33. Możliwość budowania potoków automatyzacji wdrażania i uruchamiania aplikacji zarówno w postaci infrastruktury pod aplikację, jak i budowania kontenerów oraz wdrażania i uruchamiania aplikacji, testowania aplikacji i generowania raportów z procesu
34. Dostępność kalkulatora wykorzystania usługi pozwalającego na oszacowanie kosztów wykorzystania zakupionej puli zasobów.
35. Możliwość zmiany wymaganych parametrów usługi i jej skalowania zgodnie z potrzebami.
36. Możliwość automatycznego skalowania mocy obliczeniowej usług.
37. Płatność za fizyczne wykorzystanie usług z możliwością ich okresowego wyłączania.

Zgodność ze standardami

1. Dostępność narzędzi wspomagających migrację aplikacji i danych zarówno ze środowisk własnych do usługi, jak i z usługi na dowolną inną platformę opartą o standard serwerów x64, a więc pozwalających na przeniesienie usług w przypadku podjęcia takiej decyzji.
2. Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych standardów przemysłowych, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy, potwierdzonych aktualnymi wynikami audytów, w szczególności:
   - ISO 27001, ISO 27002, ISO 27017, ISO 27018
   - SOC 1, SOC 2, SOC 3
   - Open Authentication Standard – OAuth

   W zakresie interoperacyjności:
   - HTTP(S) - TLS
   - Docker
   - REST API

W zakresie programowania:
- Java
- .NET
- PHP
- Python
- Node.js
- Wsparcie narzędziowe w Visual Studio i Eclipse

3. Wsparcie usługi dla standardowych rozwiązań OpenSource takich jak WordPress, Joomla, Drupal, OrchardCMS, MediaWiki, phpBB. Dostępność w ramach usługi predefiniowanych obrazów z tym oprogramowaniem.

Dostępność systemów i ich bezpieczeństwo

1. Usługa powinna zapewniać SLA na wszystkie swoje usługi (łącznie z pojedynczą instancją maszyny wirtualnej) na poziomie minimum 99,9%
2. Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach.
3. Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
4. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
5. Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
6. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
7. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego.
8. Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
9. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
10. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN)
11. Wbudowane mechanizmy zabezpieczające przez atakami DDoS,

12. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 500 km, znajdujące się na terenie Unii Europejskiej
13. Silnik rekomendacji zabezpieczeń infrastruktury oparty o algorytmy nauczania maszynowego
14. Dostępność usługi umożliwiającej przechowywanie certyfikatów, haseł dostępu zgodnie ze standardem FIPS 140-2 poziomu 2
15. Gradacja zakresu uprawnień i budowa konfigurowalnych zasad i ról dostępu do środowiska do poziomu pojedynczych kart sieciowych, dysków czy zarządzania uprawnieniami (tzw. RBAC, Role-Based Access Control)
16. Dostępność usługi katalogu tożsamości i przynależności użytkowników do grup wspierający OAuth2 oraz pojedynczego logowania, umożliwiający budowanie logowania przy pomocy usługodawców firm trzecich.
17. Oba centra danych powinny posiadać przynajmniej trzy z wymienionych certyfikacji: TIER-III, UK G-Cloud, ENISA IAF, SOC 1, SOC 2
18. Zamawiający wymaga dostępności następujących mechanizmów bezpieczeństwa w ramach usługi:
    - Bramki VPN.
    - Obsługi IPSec.
    - Akceleracji SSL.
    - Firewalla warstwy aplikacyjnej – WAF
    - Load balancera wspierającego Cookie Affinity
    - Systemu przeciwdziałania włamaniom – IPS.
    - Systemu wykrywania włamań - IDS.
    - Zasoby ludzkie w zakresie utrzymania usługi realizacji zadania prewencji, identyfikacji zagrożeń oraz natychmiastowe reagowanie na wszelkie incydenty bezpieczeństwa IT.
19. Posiadanie przez producenta centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.

Zgodność z obowiązującym prawem Polskim i Unijnym

1. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
2. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów członkowskich Unii Europejskiej.
3. Zobowiązania umowne potwierdzające zgodność z RODO,
4. Zapewnienie przetwarzania danych osobowych zgodnie z wymaganiami przepisów prawa a w szczególności w zakresie ochrony danych osobowych w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO),
5. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
6. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.
7. Gwarancja usunięcia danych Zamawiającego z usługi po zakończeniu umowy.
8. Gwarancja braku dostępu do danych Zamawiającego w usłudze, z wyłączeniem działań serwisowych wykonywanych wyłącznie przez uprawnione osoby z organizacji Producenta usługi.

V. <u>Opis wymaganych minimalnych funkcjonalności oprogramowania Microsoft Windows Server Datacenter (</u>Win Server DC Core ALng LSA 16L) z Software Assurance

6 sztuk nieograniczonej czasowo licencji oprogramowania dla systemu operacyjnego Win Server DC Core ALng LSA 16L z Software Assurance ważnym od dostarczenia do 30.06.2028 r.

lub równoważnego z możliwością przeniesienia licencji na inny serwer tego samego producenta

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.

2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   - pozwalają na zmianę rozmiaru w czasie pracy systemu,
   - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym)
   - prosty wgląd w poprzednie wersje plików i folderów,
   - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez
12. NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
13. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
16. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
17. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
18. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
19. Mechanizmy logowania w oparciu o:
   - Login i hasło,
   - Karty z certyfikatami (smartcard),
   - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
20. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
21. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
22. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
23. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
24. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
25. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
26. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

  - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
  - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
  - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- Zdalna dystrybucja oprogramowania na stacje robocze,
- Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
- Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  - Dystrybucję certyfikatów poprzez http,
  - Konsolidację CA dla wielu lasów domeny,
  - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
  - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- Szyfrowanie plików i folderów.
- Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
- Serwis udostępniania stron WWW.
- Wsparcie dla protokołu IP w wersjach 4 oraz 6 (IPv4; IPv6).
- Wsparcie dla algorytmów Suite B (RFC 4869).
- Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

- Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
- Obsługi 4-KB sektorów dysków
- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
  - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
  - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji poprzez skrypty.

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

VI. <u>Opis wymaganych minimalnych funkcjonalności oprogramowania Microsoft Windows Server Datacenter (</u>Win Server DC Core ALng LSA 2L) z Software Assurance

144 sztuk nieograniczonej czasowo licencji oprogramowania dla systemu operacyjnego Win Server DC Core ALng LSA 2L z Software Assurance ważnym od dostarczenia do 30.06.2028 r.

lub równoważnego z możliwością przeniesienia licencji na inny serwer tego samego producenta

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania 512 logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   - pozwalają na zmianę rozmiaru w czasie pracy systemu,
   - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym)
   - prosty wgląd w poprzednie wersje plików i folderów,
   - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   - umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez
12. NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
13. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
14. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
15. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
16. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
   - Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
   - Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
17. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
18. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
19. Mechanizmy logowania w oparciu o:
   - Login i hasło,
   - Karty z certyfikatami (smartcard),
   - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
20. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
21. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
22. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
23. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
24. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
25. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
26. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
   - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
   - Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach,

pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
  - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
  - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
  - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
- Zdalna dystrybucja oprogramowania na stacje robocze,
- Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
- Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  - Dystrybucję certyfikatów poprzez http,
  - Konsolidację CA dla wielu lasów domeny,
  - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
  - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- Szyfrowanie plików i folderów.
- Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- Możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.
- Serwis udostępniania stron WWW.
- Wsparcie dla protokołu IP w wersjach 4 oraz 6 (IPv4; IPv6).
- Wsparcie dla algorytmów Suite B (RFC 4869).
- Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
- Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
  - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
  - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
  - Obsługi 4-KB sektorów dysków
  - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
  - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
  - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji poprzez skrypty.

Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

VII. Warunki równoważności

W przypadku zaoferowania produktów lub usług z nimi związanych równoważnych względem wyspecyfikowanych przez Zamawiającego w Opisie Przedmiotu Zamówienia, Wykonawca będzie zobowiązany na swoją odpowiedzialność i swój koszt udowodnić do szczegółowego opisu sposobu spełnienia warunków równoważności przez oferowany produkt, w szczególności w zakresie:

1) warunków licencji i sublicencji w każdym aspekcie licencjonowania /sublicencjonowania, które nie mogą być gorsze niż określone w OPZ,

2) funkcjonalności produktu, która nie może być gorsza od funkcjonalności produktu wymienionego w OPZ, która opisana jest w pkt. I Przedmiot zamówienia.

3) pełnej współpracy z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie, zapewnienia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności produktu równoważnego z produktami Microsoft,

4) warunków i zakresu usług wsparcia technicznego produktu równoważnego, które muszą być nie gorsze niż dla produktów Microsoft.