Załącznik nr 1

WIS.261.32.2023.AM

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Nazwa zadania:

**Dostawa standardowego oprogramowania komputerowego dla Regionalnej Dyrekcji Ochrony Środowiska w Bydgoszczy**

1. Kod i nazwa zamówienia według Wspólnego Słownika Zamówień (CPV): 48000000-8 – pakiety oprogramowania i systemy informatyczne.
2. Przedmiotem zamówienia jest dostawa standardowego oprogramowania komputerowego dla Regionalnej Dyrekcji Ochrony Środowiska w Bydgoszczy: 1 licencji Windows Server 2022 DataCenter 16 Core lub oprogramowania równoważnego. Zamówienie obejmuje, przez okres minimum 5 lat od dnia podpisania protokołu odbioru, wsparcie do oprogramowania, w ramach którego Zamawiający zostanie uprawniony do pobierania poprawek i aktualizacji w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z oprogramowania.
3. Licencja nie może posiadać ograniczeń czasowych, musi pochodzić z oficjalnego kanału dystrybucji. Zakup licencji oprogramowania jest uzupełnieniem stanu licencyjnego oprogramowania eksploatowanego w środowisku serwerowym: Windows Server 2012, Windows Server 2016, Windows Server 2019. Licencja musi pozwalać na swobodne przenoszenie pomiędzy serwerami (np. w przypadku wymiany sprzętu), które są w posiadaniu Zamawiającego i nie może być dedykowana tylko do jednego producenta sprzętu serwerowego.
4. W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter, Zamawiający wymaga dostarczenia licencji dla 10 serwerów, oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga aby produkt równoważny spełniał niżej wymienione wymagania:

 1) Współpraca z procesorami o architekturze x86 – 64bit.

2) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.

3) Możliwość budowania klastrów składających się z 64 węzłów.

4) Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni.

5) Praca w roli klienta domeny Microsoft Active Directory.

6) Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.

7) Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.

8) Możliwość uruchomienia roli klienta i serwera czasu (NTP).

9) Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.

10) Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.

11) Możliwość uruchomienia roli serwera stron WWW.

12) W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

13) W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.

14) Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

15) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

16) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.

17) Wbudowane wsparcie instalacji i pracy na wolumenach, które:

a) pozwalają na zmianę rozmiaru w czasie pracy systemu,

b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

d) umożliwiają zdefiniowanie list kontroli dostępu (ACL).

18) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość

19) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

20) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

21) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

22) Możliwość wykorzystania standardu http/2.

23) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

24) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

25) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

26) Mechanizmy logowania w oparciu o: a) login i hasło,

a) karty z certyfikatami (smartcard),

b) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).

27) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:

a) określonych grup użytkowników,

b) zastosowanej klasyfikacji danych,

c) centralnych polityk dostępu w sieci,

d) centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.

28) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

29) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

30) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

31) Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji

w dokumentach (Digital Rights Management).

32) Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

33) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a) podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

b) 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:

• podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

• 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.,

c) zdalna dystrybucja oprogramowania na stacje robocze,

d) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,

e) 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.

f) szyfrowanie plików i folderów,

g) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),

h) szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,

i) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,

j) serwis udostępniania stron WWW,

k) wsparcie dla protokołu IP w wersji 6 (IPv6),

l) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),

n) możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

o) możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover

z jednoczesnym zachowaniem pozostałej funkcjonalności.

p) mechanizmy wirtualizacji mające 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,

• możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

q) możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.

r) wsparcie dla rozwiązania Kubernetes.

s) 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.

t) wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).

u) mechanizmy deduplikacji i kompresji na wolumenach.

v) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

w) mechanizm konfiguracji połączenia VPN do platformy Azure.

x) wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.

y) mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.

z) możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).