

## Załącznik nr 1 do projektu umowy

### Szczegółowy Opis Przedmiotu Zamówienia

#### I. Opis istniejącego środowiska zamawiającego

##### 1. Opis ogólny

Zamawiający posiada środowisko serwerowe oparte na systemach operacyjnych Microsoft Windows Server.

##### 2. Specyfikacja istniejącego środowiska

Zamawiający posiada pulę licencji dla instytucji publicznych/rządowych (Government). Poniższy zakres dostawy obejmuje zakup nowych licencji wraz z pakietami wsparcia (Software Assurance) dla środowiska Microsoft Windows Server dla instytucji publicznych/rządowych (Government).

#### II. Wymagania

##### 1. Zakres dostawy

1. Dostawa licencji dla instytucji publicznych/rządowych (Government) wskazanych w Tabeli 1 wraz z pakietami wsparcia (Software Assurance). Okres obowiązywania pakietów wsparcia (Software Assurance) musi wynosić co najmniej 36 miesięcy.

Lp	Nazwa ref.	Kod ref.	Ilość	Rodzaj
1	Win Server Datcr Core 16 LSA	AAA-90053	6	Government
2	Win Server Datcr Core 2 LSA	AAA-30380	24	Government

Tabela 1

##### 2. Wymagania techniczne i organizacyjne

1. Okres obowiązywania wszystkich pakietów wsparcia (Software Assurance) dla dostarczonych licencji z Tabeli 1 musi wynosić co najmniej 36 miesięcy.
2. Produkty muszą być zamówione w ramach programu MPSA na podstawie podpisanej przez Zamawiającego umowy z firmą Microsoft. Dostarczone pakiety wsparcia i licencje muszą zostać przypisane do konta Microsoft Zamawiającego (konto Gminy Wrocław). Numer konta zostanie przekazany Wykonawcy po rozstrzygnięciu postępowania i wyłonieniu Wykonawcy.
3. Na potrzeby odbioru zostanie zweryfikowane czy na portalu licencyjnym, na koncie Zamawiającego, pojawiła się informacja zakupie licencji wymienionych w Tabeli 1.

##### 3. Cechy równoważnego oprogramowania typu Microsoft Windows Server Datacenter

W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w Opisie Przedmiotu Zamówienia,

Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w SOPZ, w szczególności w zakresie:

- 1) Współpraca z procesorami o architekturze x64.
- 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 obsługiwać serwer fizyczny zgodnie z wypisanymi wcześniej wymaganiami dla licencji .
- 5) Praca w roli klienta domeny Microsoft Active Directory.
- 6) Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2022.
- 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 instalacji i użytkowania systemu operacyjnego na nieograniczonej ilości maszyn wirtualnych w ramach licencjonowanego hosta.
- 14) W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
- 15) 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).
- 16) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- 17) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- 18) 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).
- 19) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- 20) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- 21) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.
- 22) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- 23) Możliwość wykorzystania standardu http/2.
- 24) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- 25) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
- a) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
  - b) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
- 26) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- 27) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
- 28) Mechanizmy logowania w oparciu o:
- a) login i hasło,
  - b) karty z certyfikatami (smartcard),
  - c) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
- 29) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
- a) kreślonych grup użytkowników,
  - b) zastosowanej klasyfikacji danych,
  - c) centralnych polityk dostępu w sieci,

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

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

31) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

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

33) Dostępny, pochodzący od producenta systemu, serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

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

35) 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 stacjoroboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

a. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

b. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

c. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

d. 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:

a. Dystrybucję certyfikatów poprzez http,

b. Konsolidację CA dla wielu lasów domeny,

- c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- d. 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) Wsparcie dla algorytmów Suite B (RFC 4869).
- m) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
- n) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
- o) Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- p) Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- q) Mechanizmy wirtualizacji mające wsparcie dla:
  - a. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
  - b. obsługi ramek typu jumbo frames dla maszyn wirtualnych.
  - c. obsługi 4-KB sektorów dysków,
  - d. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
  - e. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

- f. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunkmode)
  - g.możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
  - r) Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
  - s) Wsparcie dla rozwiązania Kubernetes.
  - t) 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.
  - u) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
  - v) Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
  - w) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
  - x) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
  - y) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF
  - z) Mechanizm konfiguracji połączenia VPN do platformy Azure.
  - aa) Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
  - bb) Mechanizmy pozwalające na blokadę dostępu nieznanym procesom do chronionych katalogów.
  - cc) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
  - dd) Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Enterprise).
- 36) W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt

przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania SOPZ.

37) Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.

#### **4. Gwarancja, wsparcie i dokumentacja**

1. Wsparcie musi być świadczone bezpośrednio przez producenta zgodnie z SLA w ramach programu Software Assurance lub równoważnego.
2. Zakres i warunki wsparcia muszą być dostarczone do umowy oraz powinny zawierać jedynie informacje o produktach, które są przedmiotem tego zamówienia.