

OPIS PRZEDMIOTU ZAMÓWIENIA
w postępowaniu pn. Dostawa oprogramowania w ramach projektu
grantowego „Cyberbezpieczny Samorząd”

I. Część 1 zamówienia

1. Oprogramowanie przeciwdziałające wyciekowi danych – 80 sztuk.

1. System operacyjny:
 1. Windows 10 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
 2. Windows 11 (64-bit) z wszystkimi aktualizacjami zabezpieczającymi
 3. MacOS 12 lub nowszy.
- 2) Serwer administracyjny musi obsługiwać instalację na systemach:
 1. Windows Server 2016 (64-bit) i nowszych.
- 3) Serwer administracyjny musi obsługiwać bazy danych:
 1. MS SQL Server 2016 lub nowsze,
 2. MS SQL Express, c. AzureSQL S3 lub nowsze.
- 4) Pomoc i dokumentacja programu dostępne w języku angielskim.
- 5) Konsola administracyjna i komunikaty klienta muszą być w języku polskim.
- 6) Konsola zarządzająca musi umożliwiać pobranie pliku instalacyjnego agenta.
- 7) Serwer administracyjny musi umożliwiać instalację/deinstalację zdalnego klienta na stacjach roboczych.
- 8) Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym.
- 9) Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia.
- 10) Serwer administracyjny musi umożliwiać zarządzanie za pośrednictwem konsoli.
- 11) System musi mieć możliwość konfiguracji automatycznej konserwacji dla bazy danych, usuwając najstarsze informacje, gdy rozmiar bazy osiągnie skonfigurowany limit.
- 12) Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.
- 13) Administrator musi mieć możliwość aby tworzyć, usuwać i konta administratorów w konsoli programu.
- 14) Administrator musi mieć możliwość przypisywania i odbierania uprawnień do wybranych
- 15) modułów programu, podzielonych na ustawienia (konfiguracja modułu) i logi (wyświetlanie logów modułu).
- 16) Serwer musi synchronizować użytkowników i stacje robocze z domeną Active Directory.
- 17) Administrator musi móc wymusić synchronizację ustawień i logów między stacją roboczą a serwerem w czasie rzeczywistym.
- 18) Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.
- 19) Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.

- 20) Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.
- 21) Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.
- 22) Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.
- 23) Dashboardsy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.
- 24) Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.
- 25) Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.
- 26) Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.
- 27) Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przysyłanie komunikatorami itp.
- 28) Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.
- 29) Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.
- 30) Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.
- 31) Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.
- 32) Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.
- 33) System musi ochraniać pocztę e-mail Microsoft 365, sprawdzając każdą wiadomość e-mail wysłaną przez użytkowników Microsoft 365.
- 34) System musi ochraniać pliki w Microsoft 365, kontrolując aktywność plików w Microsoft SharePoint, Microsoft OneDrive dla Firm i Microsoft Teams.
- 35) System musi wykorzystywać mechanizm OCR (optical character recognition), aby wykrywać poufne treści w obrazach, zdjęciach i zeskanowanych dokumentach
- 36) System musi posiadać możliwość integracji z systemami do analizy danych (PowerBI, Tableau, etc.)
- 37) System musi zapewniać możliwość zarządzanie szyfrowaniem dysków twardych oraz urządzeń wymiennych.

2. Licencje dostępne – 20 sztuk.

1. Licencje dostępne na użytkownika
 - Wymagana licencja typu Cal User OEM do systemu Windows Server 2025 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.
2. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2025 na użytkownika:
 - Licencja dostępowa dla użytkownika umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu User Cal z wdrożoną rolą Active Directory

3. Licencje dostępne – 15 sztuk.

1. Licencje dostępne na urządzenie

- Wymagana licencja typu Device CAL OEM do systemu Windows Server 2025 (z niniejszego zamówienia) lub równoważne, jeśli oprogramowanie równoważne takich licencji wymaga.
2. Opis równoważności dla funkcjonalności dotyczące wymaganego przez Zamawiającego oprogramowania równoważnego do Windows Server 2025 na urządzenie:
- Licencja dostępowa na urządzenie umożliwiające podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2025 typu Device CAL z wdrożoną rolą Active Directory.
 - Oprogramowanie równoważne musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania, przez nieograniczoną liczbę użytkowników korzystających ze wskazanej liczby urządzeń, funkcjonalności serwerowych systemów operacyjnych (z wyłączeniem dostępu terminalowego).

4. Oprogramowanie serwera – 4 sztuki.

Licencje systemu operacyjnego Microsoft Windows Server 2025 Datacenter 16-core lub oprogramowania równoważnego nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji. Licencje nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

RÓWNOWAŻNOŚĆ:

1. Warunki równoważności dla licencji systemu Microsoft Windows Server 2025 Datacenter.

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2025 Datacenter. 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 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:

1. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 2. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 3. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 4. 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 zaporę internetową (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,
1. karty z certyfikatami (smartcard),
 2. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:
1. określonych grup użytkowników,
 2. zastosowanej klasyfikacji danych,
 3. centralnych polityk dostępu w sieci,
 4. 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:
1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
 2. 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.,
3. zdalna dystrybucja oprogramowania na stacje robocze,
 4. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
 5. 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.
 6. szyfrowanie plików i folderów,
 7. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
 8. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
 9. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
 10. serwis udostępniania stron WWW,
 11. wsparcie dla protokołu IP w wersji 6 (IPv6),
 12. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
 13. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
 14. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
 15. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
 16. 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.
 16. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
 17. wsparcie dla rozwiązania Kubernetes.
 18. 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.
 19. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
 20. mechanizmy deduplikacji i kompresji na wolumenach.
 21. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

Dofinansowane przez
Unię Europejską



22. mechanizm konfiguracji połączenia VPN do platformy Azure.
23. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
24. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
25. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

Wspólny Słownik Zamówień:

CPV 72268000-1 Usługi dostawy oprogramowania

CPV 72263000-6 Usługi wdrażania oprogramowania

Zamówienie będzie wykonane w miejscu siedziby zamawiającego. Przedmiot umowy będzie dostarczany przez Wykonawcę do miejsc wskazanych przez Zamawiającego w zakresie dostawy sprzętu/oprogramowania/licencji.

Wójt Gminy Gostynin

/-/ Renata Kędzierska

.....

Zatwierdził: