

Załącznik nr 1: Szczegółowy opis parametrów technicznych i funkcjonalności

I. Cel:

Zamawiający planuje zakup pakietów subskrypcji, zasobów chmury obliczeniowej oraz licencji oprogramowania serwerowego wraz ze wsparciem Software Assurance Microsoft albo pakietów subskrypcji, zasobów chmury obliczeniowej oraz licencji oprogramowania serwerowego wraz ze wsparciem technicznym równoważnych do Microsoft zwanych dalej Oprogramowaniem, dla jednostek organizacyjnych Państwowej Inspekcji Pracy.

W ramach realizacji zamówienia, Wykonawca dostarczy następujące oprogramowanie Microsoft:

LP.	Nazwa produktu	Numer katalogowy	Liczba
1	Defender Endpoint Server Sub	1NZ-00004	500
2	M365 E5 Security Sub Per User	PEJ-00002	1200
3	EMS E5 SU EMS E3 Per User	CE6-00004	1560
4	Defender Endpoint P2 Sub Per User	QLS-00003	1560
5	Azure prepayment	6QK-00001	6
6	CIS Suite Datacenter Core ALng LSA 16L	9GS-00128	4

Zamawiający informuje, że:

- posiada środowisko chmurowe (tenant) na platformie Microsoft, na którym musi być zapewniona kontynuacja subskrypcji oprogramowania Microsoft;
- posiada umowę Enterprise Agreement o numerze 47951772, której ważność kończy się 31 grudnia 2026 roku. Zamawiający nie dopuszcza dostarczenia oprogramowania firmy Microsoft w ramach innej umowy niż posiadanej Enterprise Agreement.

W ramach w/w umowy posiada pakiet subskrypcji EMS E3 ALng Sub Per User (numer katalogowy AAA-10732), O365 E3 FUSL EEA Sub Per User (numer katalogowy 84Q-00004) oraz Teams EEA Sub Per User (numer katalogowy 8Y8-00001) w odpowiedniej ilości.

Zamawiający wymaga dostarczenia licencji i/lub aktywacji subskrypcji Microsoft w terminie 7 dni kalendarzowych od dnia podpisania umowy ważnych do końca posiadanej umowy Enterprise Agreement. Zamawiający wymaga dostarczenia licencji w ciągu 7 dni kalendarzowych od podpisania umowy

II. Zamawiający dopuszcza zaoferowanie pakietów równoważnych do Oprogramowania.

Jeżeli Zamawiający określił w OPZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych albo równoważnych, spełniających poniższe warunki równoważności.

1. Zamawiający posiada licencje na oprogramowanie firmy Microsoft oraz wdrożone systemy informatyczne, które korzystają oraz współpracują z innymi rozwiązaniami firmy Microsoft tj. Active Directory Domain Services, Microsoft Azure, Microsoft Windows 10/11/Server 2016, Server 2019, Server 2022, Server 2025, Microsoft Office w różnych wersjach, SharePoint oraz systemy innych producentów.
2. W przypadku dostarczania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w OPZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone w OPZ, w szczególności w zakresie:
  - warunków licencji/sublicencji w każdym aspekcie licencjonowania/sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania,
  - funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w rozdziale III „Opis wymagań minimalnych dla licencji równoważnej” oraz w rozdziale I, gdzie kody produktu wzorcowego definiują funkcjonalności, jakie musi spełnić produkt równoważny,
  - oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z innymi systemami oraz oprogramowaniem Microsoft oraz innych producentów funkcjonującym u Zamawiającego, oraz w żaden sposób nie naruszać ich warunków licencyjnych,
  - oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
  - oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
  - oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem firmy Microsoft tj. Active Directory Domain Services, Microsoft Azure,

Microsoft Windows 10/11/Server 2016, Server 2019, Server 2022, Server 2025, Microsoft Office w różnych wersjach, SharePoint oraz systemy innych producentów, które funkcjonują u Zamawiającego,

3. W przypadku zaproponowania oprogramowania równoważnego Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego oprogramowania. 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 być dłuższa niż 7 godzin.
4. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona konfiguracji, transferu wiedzy oraz danych w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
5. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje 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 równoważnego.
6. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia/gwarancji producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
7. Oprogramowanie równoważne dostarczone przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.
8. W przypadku dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:
  - dostarczyć i uruchomić (wdrożyć) oprogramowanie równoważne w środowisku systemowo-programowym Zamawiającego dla wszystkich użytkowników w terminie do 14 dni od dnia podpisania Umowy,
  - dostarczyć wszelkie dodatkowe licencje - niezbędne do prawidłowego funkcjonowania oprogramowania równoważnego,

- przeprowadzić pełną migrację kont, oraz wszystkich danych z obecnie używanego systemu na system równoważny.

III. Opis wymagań minimalnych dla licencji równoważnej:

Zamawiający wymaga dostarczenia licencji oraz instalacji i migracji obecnego środowiska w terminie 14 dni roboczych od podpisania umowy.

Zamawiający wymaga, aby oprogramowanie równoważne do pakietów wymienionych w pozycjach od 1 do 4 tabeli wskazanej w rozdziale I OPZ, spełniało niżej wymienione wymagania:

Wymagania funkcjonalne:

1. Tożsamość i zarządzanie dostępem:

- a) wykrywanie i reagowanie na ryzyko związane z kontami użytkowników,
- b) konfiguracja polityk dostępu opartych na ryzyku, urządzeniach i lokalizacji,
- c) zarządzanie uprawnieniami administratorów z dostępem just-in-time (JIT),
- d) wymuszanie wieloskładnikowego uwierzytelniania dla wszystkich użytkowników,
- e) umożliwienie użytkownikom samodzielnej zmiany haseł.

Zaawansowana ochrona punktów końcowych:

- a) ochrona przed zaawansowanymi zagrożeniami, takimi jak ransomware i ataki zero-day,
- b) automatyczna analiza i remediacja zagrożeń na urządzeniach,
- c) zarządzanie podatnościami w organizacji i rekomendacje dotyczące poprawy bezpieczeństwa,
- d) integracja z Microsoft Intune w celu egzekwowania polityk bezpieczeństwa;

Ochrona poczty i współpracy:

- a) ochrona przed phishingiem, malware i atakami Business Email Compromise (BEC),
- b) sandboxing załączników i skanowanie linków w czasie rzeczywistym (Safe Links, Safe Attachments),
- c) zautomatyzowane dochodzenia i reakcje na incydenty bezpieczeństwa,
- d) monitorowanie i analiza zagrożeń w wiadomościach e-mail oraz komunikatorach.

Ochrona danych i zgodność:

- a) klasyfikacja i szyfrowanie dokumentów w oparciu o etykiety poufności,

- b) ochrona przed wyciekiem danych w e-mailach, komunikatorach,
  - c) wykrywanie podejrzanych działań użytkowników wewnątrz organizacji,
  - d) zaawansowane monitorowanie aktywności użytkowników i administratorów.
2. Zarządzanie i monitoring:
- a) możliwość monitorowania i raportowania incydentów bezpieczeństwa w czasie rzeczywistym,
  - b) automatyzacja reakcji na zagrożenia.
3. Usługa bezpieczeństwa informacji, która pozwala na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania. Zamawiający informuje, iż Zamawiającemu zależy, aby w oprogramowaniu SPL były widoczne lub odczytywalne informacje/logi z oferowanego produktu. Możliwość przekierowania w bezpieczny sposób logów do SPL lub inny sposób pozwalający na odczytanie logów generowanych przez O365 np. poprzez bezpieczne API i aplikacje/addon w SPL. Dobór rozwiązania pozostawiamy Wykonawcy, jednakże Zamawiający preferuje wykorzystanie bezpiecznego API.
4. ATP (Advanced Threat Protection) usługa skanowania załączników wiadomości e-mail, dokumentów przechowywanych w aplikacjach Zamawiającego w celu lokalizowania i usuwania złośliwej zawartości. Ponadto ATP ma umożliwiać skanowanie adresów URL w wiadomościach e-mail, aby upewnić się, że są one bezpieczne.

Zamawiający wymaga, aby produkt równoważny do zasobów chmury obliczeniowej wymienionych w pozycji 5 (Azure prepayment) tabeli wskazanej w rozdziale I OPZ, spełniał niżej wymienione wymagania:

1. Subskrypcja standardowej, powszechnie dostępnej przez Internet usługi hostowanej typu COTS (Commercial Of-The-Shelf) udostępniająca skalowalną platformę i pozwalająca wykorzystać w ramach zakupionej puli zasobów – maszyny wirtualne, systemy operacyjne, silniki baz danych oraz inne aplikacje i usługi PaaS oraz IaaS spełniające poniżej opisane wymagania.
2. Pula zasobów zakupionych w pakiecie musi umożliwić wykorzystanie:
  - 2.1 Minimum 1 jednostki obliczeniowej o parametrach - 1 rdzeń procesora, 1,7 GB RAM, pod kontrolą systemu operacyjnego Windows Server lub Linux (wybrane dystrybucje),
  - 2.2 Minimum 50 GB dostępnej lokalnie redundantnej przestrzeni dyskowej,

- 2.3 Minimum 50 GB dostępnej georedundantnej przestrzeni dyskowej (odległości min. 100km między lokalizacjami),
- 2.4 Minimum 100 GB transferu danych do i z usługi miesięcznie.
- 2.5 Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług.
- 2.6 Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
- 2.7 Możliwość wyboru różnych rodzajów dysków i ich pojemności.
- 2.8 Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów, z możliwością zdalnego dostępu.
- 2.9 Komunikacja z mechanizmami zarządzania usługi poprzez REST API.
- 2.10 Możliwość przechowywania danych spełniająca następujące wymagania (opcjonalnie dostępnych w ramach usługi):
- 2.11 Wysoka skalowalność, auto-partycjonowanie, load-balancing
- 2.12 Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka
- 2.13 Wsparcie dla systemów klienckich Windows i Linux
- 2.14 Skalowalność pojedynczego zasobu pamięci 500TB
- 2.15 Replikacja danych - min. 3 kopie w ramach pojedynczej lokalizacji
- 2.16 Replikacja do innej lokalizacji oddalonej o min 100km od lokalizacji podstawowej
- 2.17 Udostępnienie zasobów pamięci poprzez REST API
- 2.18 Gotowe biblioteki programistyczne środowisk programowania: .NET, Java/Android, Node.js, PHP, Ruby, Python, PowerShell
- 2.19 Konfigurowalne usługi wyszukiwania treści w zasobach własnych i internet.
- 2.20 Konfigurowalne usługi analizy wyszukanych treści.
- 2.21 Dostępność usług umożliwiających uruchamianie aplikacji WWW w modelu gotowej do wykorzystania usługi, z utrzymywaniem przez dostawcę 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.
- 2.22 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 rozproszonej geograficznie przestrzeni magazynowej.
- 2.23 Dostępność relacyjnej i nierelacyjnej bazy danych, w tym oparte o technologię Hadoop, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
- 2.24 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%.
- 2.25 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.
- 2.26 Dostępny portal administracyjny, pozwalający na uruchamianie usług poprzez wybór spośród dostępnych usług.
- 2.27 Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci).
- 2.28 Włączenie reguł wymuszających stosowanie się do odpowiedniej nomenklatury nazewnictwa zasobów w obrębie środowiska, wymuszając wykorzystanie ustalonego modelu nazw, prefiksów dla określonych typów zasobów
- 2.29 Dostępność usług umożliwiających utworzenie prywatnego repozytorium obrazów kontenerów w standardzie zgodnym z Docker.
- 2.30 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.
- 2.31 Dostępność relacyjnych baz danych, zgodnych z MySQL i z PostgreSQL, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
- 2.32 Dostępność bazy danych typu NoSQL, oferującej API dostępne zgodne z MongoDB dostępnej jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%.
- 2.33 Przynajmniej dwa jasno zdefiniowane poziomy spójności danych dla bazy NoSQL.
- 2.34 Możliwość automatycznej dystrybucji danych pomiędzy różne regiony oraz ulokowane w nich centra obliczeniowe wraz z możliwością ręcznego jak i automatycznego przełączania replik

- 2.35      Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a dostawcą usług chmurowych w technologii opartej o światłowody.
- 2.36      Posiadanie przez dostawcę centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.
- 2.37      Akcelerowana, definiowana programowo sieć wirtualna w środowisku, wspierająca akcelerację SR-IOV, realizowana na akcelerowanych interfejsach sieciowych FPGA, do 30Gb/s.
- 2.38      Możliwość śledzenia ruchu sieciowego.
- 2.39      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.
- 2.40      Możliwość wykorzystania usług SMB 3.0 do współdzielenia plików wykorzystując szyfrowanie podczas transmisji, jako usługa.
- 2.41      Możliwość zdefiniowania szablonu maszyny wirtualnej włącznie z konfiguracją aplikacji, uruchamiania serwisów poprzez zdefiniowanie stanu oczekiwanego w postaci plików konfiguracyjnych.
- 2.42      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.
- 2.43      Przewidywalny koszt budowy i utrzymania:
  - a) Oparcie się o usługi typu subskrypcji standardowej, powszechnie dostępnej przez internet usługi hostowanej typu COTS (Commercial Of-The-Shelf) o przewidywalnym koszcie określonym jasnymi zasadami wyceny.
  - b) Dostępność kalkulatora wykorzystania usługi pozwalającego na oszacowanie kosztów wykorzystania zakupionej puli zasobów.
  - c) Możliwość zmiany wymaganych parametrów usługi i jej skalowania zgodnie z potrzebami.
  - d) Możliwość automatycznego skalowania mocy obliczeniowej usług.
  - e) Płatność za fizyczne wykorzystanie usług z możliwością ich okresowego wyłączenia.
- 2.44      Zgodność ze standardami



- a) 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.
- b) 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:
  - i) ISO 27001, ISO 27002, ISO 27017, ISO 27018
  - ii) SOC 1, SOC 2, SOC 3
  - iii) Open Authentication Standard – OAuth
- c) W zakresie interoperacyjności:
  - i) HTTP(S) - TLS
  - ii) Docker
  - iii) REST API
- d) W zakresie programowania:
  - ii) Java
  - iii) NET
  - iv) PHP
  - v) Python
  - vi) Node.js
  - vii) Wsparcie narzędziowe w Visual Studio i Eclipse
  - viii) Wsparcie usługi dla standardowych rozwiązań OpenSource takich jak WordPress, Joomla, Drupal, OrchardCMS, MediaWiki, phpBB.Dostępność w ramach usługi predefiniowanych obrazów z tym oprogramowaniem.

#### 2.45 Dostępność systemów i ich bezpieczeństwo

- a) Usługa powinna zapewniać SLA na wszystkie swoje usługi (łącznie z pojedynczą instancją maszyny wirtualnej) na poziomie minimum 99,9%.
- b) Dostępność mechanizmów pełnej rozliczalności działań użytkowników w usługach.
- 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, oddalone od siebie o co najmniej 500 km, znajdujące się na terenie Unii Europejskiej, przynajmniej jeden ośrodek przetwarzania danych na terenie Polski.
- n) Silnik rekomendacji zabezpieczeń infrastruktury oparty o algorytmy nauczania maszynowego.
- o) Dostępność usługi umożliwiającej przechowywanie certyfikatów, haseł dostępu zgodnie ze standardem FIPS 140-2 poziomu 2 lub równoważną.
- p) 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).
- q) Dostępność usługi katalogu tożsamości i przynależności użytkowników do grup wspierający OAuth2 oraz pojedynczego logowania, umożliwiający budowanie logowania przy pomocy dostawców firm trzecich.

- r) Oba centra danych powinny posiadać przynajmniej trzy z wymienionych certyfikacji: TIER-III, UK G-Cloud, ENISA IAF, SOC 1, SOC 2 lub innych, równoważnych w zakresie sposobu oceny bezpieczeństwa.
- 2.46 Zamawiający wymaga dostępności następujących mechanizmów bezpieczeństwa w ramach usługi:
- i) Bramki VPN.
  - ii) Obsługi IPSec.
  - iii) Akceleracji SSL.
  - iv) Firewalla warstwy aplikacyjnej – WAF
  - v) Load balancera wspierającego Cookie Affinity
  - vi) Systemu przeciwdziałania włamaniom – IPS.
  - vii) Systemu wykrywania włamań - IDS.
  - viii) Zasoby ludzkie w zakresie utrzymania usługi realizacji zadania prewencji, identyfikacji zagrożeń oraz natychmiastowe reagowanie na wszelkie incydenty bezpieczeństwa IT.
  - ix) Posiadanie przez dostawcę centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania.
- 2.47 Zgodność z obowiązującym prawem polskim i unijnym
- i. Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
  - ii. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów członkowskich Unii Europejskiej.
  - iii. Zobowiązania umowne potwierdzające zgodność z RODO,
  - iv. 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),
  - v. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego.
  - vi. Mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług.

- vii. Gwarancja usunięcia danych Zamawiającego z usługi po zakończeniu umowy.
- viii. Gwarancja braku dostępu do danych Zamawiającego w usłudze, z wyłączeniem działań serwisowych wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy usługi.
- ix. Gwarancja usunięcia danych w terminie do 180 dni od wygaśnięcia subskrypcji i zakończenia umowy.

Dla pozycji 6 tabeli wskazanej w rozdziale I OPZ (dotyczy: CIS Suite Datacenter Core ALng LSA 16L), Zamawiający wymaga, aby oprogramowanie równoważne spełniało poniższe wymagania:

- a) Licencje muszą pozwalać na przenoszenie pomiędzy serwerami fizycznymi jak również hostami farmy serwerów wirtualnych.
- b) Licencje mają być niewyłączne, nieodwołalne, nieograniczone terytorialnie - umożliwiające korzystanie z oprogramowania w każdej lokalizacji Zamawiającego na terytorium Polski, a także za granicą bez dodatkowych opłat lub ograniczeń terytorialnych
- c) Licencje muszą pochodzić z legalnego źródła tj. musi pochodzić od producenta, oficjalnego partnera lub autoryzowanego dystrybutora
- d) Licencje muszą być zgodne z przepisami prawa polskiego, w tym ustawy o prawie autorskim i prawach pokrewnych
- e) Licencja nie może zawierać zobowiązań do dodatkowych opłat za działania związane z użytkowaniem licencji przez Zamawiającego w okresie jej trwania ,
- f) Licencja nie może przewidywać korzystania z oprogramowania od dodatkowych warunków,
- g) Licencjonowanie musi uwzględniać dostarczanie przez producenta oprogramowania poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania i prawo do bezpłatnej ich instalacji w okresie przynajmniej 5 lat od daty publikacji oprogramowania przez producenta tego oprogramowania.
- h) Wymagane jest zapewnienie możliwości korzystania z wcześniejszych wersji Zamawianego oprogramowania (umożliwia downgrading) i korzystania z kopii zamiennych (możliwość kopiowania oprogramowania na wiele urządzeń przy wykorzystaniu jednego standardowego obrazu uzyskanego z nośników dostępnych w programach licencji grupowych), z prawem do wielokrotnego użycia jednego obrazu dysku w procesie instalacji i tworzenia kopii zapasowych.

- i) Licencjonowane uruchomienie dowolnej liczby serwerów Windows Server na każdym węźle klastra.
- j) Wysoka dostępność (HA) dla zainstalowanych maszyn wirtualnych (VM).
- k) Automatyczna zmiana ustawień pamięci RAM a także dysków podczas pracy maszyny wirtualnej.
- l) Przenoszenie uruchomionych maszyn wirtualnych pomiędzy węzłami klastra z zachowaniem ciągłości i integralności jej pracy (live migration).
- m) Mechanizm szyfrowania dysków.
- n) Współpraca z procesorami o architekturze x86 – 64bit.
- o) Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
- p) Możliwość budowania klastrów składających się z 64 węzłów.
- q) Praca w roli klienta domeny Microsoft Active Directory.
- r) Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2025.
- s) Możliwość federowania klastrów typu failover w zespół klastrów z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
- t) Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- u) Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
- v) W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.
- w) W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
- x) 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).
- y) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- z) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.

Wbudowane wsparcie instalacji i pracy na wolumenach, które:



- i. pozwalają na zmianę rozmiaru w czasie pracy systemu,
- ii. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- iii. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- iv. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

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

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

Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.

Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

Możliwość wykorzystania standardu http/2.

Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

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

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

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).

Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:

- i) określonych grup użytkowników,
- ii) zastosowanej klasyfikacji danych,
- iii) centralnych polityk dostępu w sieci,
- iv) centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.

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

Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

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





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

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:
  - i) połączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
  - ii) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
  - iii) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
  - iv) bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o i
  - v) OS,
  - vi) Windows 10 i Windows 11
  - vii) zdalna dystrybucja oprogramowania na stacje robocze,
  - viii) praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. użytkowników,

Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:

- a) Dystrybucję certyfikatów poprzez http,
- b) Konsolidację CA dla wielu lasów domeny,
- c) Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
- d) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509,
- e) szyfrowanie plików i folderów,
- f) szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
- g) szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,

- h) możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
- i) serwis udostępniania stron WWW,
- j) wsparcie dla protokołu IP w wersji 6 (IPv6),
- k) wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- l) wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
- m) możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
- n) możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności,

Mechanizmy wirtualizacji mające wsparcie dla:

- i) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
- ii) obsługi ramek typu jumbo frames dla maszyn wirtualnych,
- iii) obsługi 4-KB sektorów dysków,
- iv) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
- v) możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego,
- vi) możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów,
- vii) wsparcie dla rozwiązania Kubernetes,
- viii) 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,
- ix) wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath),
- x) mechanizmy deduplikacji i kompresji na wolumenach,

- xi) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
- xii) mechanizm konfiguracji połączenia VPN do platformy Azure,
- xiii) wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu,
- xiv) mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów,

Licencje na oprogramowanie muszą uprawniać do uruchomienia wymaganych serwerów zarządzających wraz z dedykowaną bazą danych.

System zarządzania musi uprawniać do zarządzania środowiskiem fizycznym i maszynami wirtualnymi w ilości określonej w warunkach szczegółowych na nim posadowionych w zakresie wszystkich wymienionych poniżej funkcji:

- a) Moduł monitorowania stanu, wydajności i wykorzystania infrastruktury, aplikacji i procesów.
- b) Moduł automatyzacji wykonywania zadań w centrum przetwarzania, pozwalający w prosty sposób wykorzystać, łączyć i automatyzować wykonanie natywnych skryptów PowerShell.
- c) Moduł powoływania maszyn wirtualnych na platformie Windows Server i zarządzania nimi w ramach centrum przetwarzania, umożliwiający zarządzanie wykorzystaniem sieci, przestrzeni dyskowych, przetwarzania i uprawnionego dostępu.
- d) Moduł ochrony danych poprzez ich bezpieczne składowanie (backup), zarządzanie składowanymi danymi, odtwarzanie danych produkcyjnych. Ma umożliwiać wykorzystanie dla chmury prywatnej, maszyn fizycznych, urządzeń klienckich i aplikacji serwerowych.
- e) Moduł wsparcia technicznego dla rozwiązywania problemów technicznych, zarządzania zmianą konfiguracji i zarządzania cyklem życia.
- f) Moduł zarządzania serwerami i komputerami klasy PC w środowisku własnej organizacji, pozwalający na wykonywanie aktualizacji oprogramowania i zarządzanie aktualizacjami, planowanie i wdrażanie polityk konfiguracyjnych i bezpieczeństwa oraz monitorujący status systemów.
- g) Integracja umożliwiająca przekazywanie alertów z monitoringu do kanału Microsoft Teams.
- h) Możliwość oparcia dostępu do narzędzi w oparciu o rolę administratora w organizacji.
- i) Wsparcie dla zarządzania hostami Azure Stack HCI i VMware 7.0.



- j) Licencja uprawnia do zarządzania nieograniczoną ilością maszyn wirtualnych.

Wykonawca ponosi odpowiedzialność cywilną za ewentualne roszczenia osób trzecich wynikające z naruszenia praw autorskich w związku z dostarczeniem licencji.

Zamówienie dofinansowane w ramach projektu pn. „Cyberbezpieczeństwo w PIP”, Program: Krajowy Plan Odbudowy i Zwiększania Odporności; Priorytet: C3 Cyberbezpieczeństwo; Działanie: C3.1.1. Cyberbezpieczeństwo - CyberPL – numer porozumienia o powierzenie grantu KPOD.05.10- CR.01-001/24/0036/ KPOD.05.10-CR.01-001/25/2025.