ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa przedmiotu zamówienia:

Dostawa pakietów subskrypcyjnych w zakresie usługi publicznej chmury obliczeniowej na okres 36 miesięcy.

II. Oznaczenie przedmiotu zamówienia wg CPV:

48000000-8 Pakiety oprogramowania i systemy informatyczne

III. Przedmiot zamówienia

1. Przedmiotem zamówienia jest dostawa pakietów subskrypcyjnych w zakresie usługi publicznej chmury obliczeniowej (zwanych dalej: „Rozwiązaniem") aktywnych przez okres 36 miesięcy od dnia ich dostarczenia Zamawiającemu.
   1) Zamawiający informuje, że w celu realizacji zamówienia konieczne jest uprzednie podpisanie aneksu do rejestracji Microsoft Server and Cloud (SCE) do umowy Enterprise Agreement, pozwalającego na zakup wymienionej w zamówieniu liczby pakietów Azure Prepayment. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca może pominąć etap zawarcia aneksu, o ile dostawa rozwiązania równoważnego tego nie wymaga, z zastrzeżeniem osiągnięcia funkcjonalności opisanych w tabeli produktów w pkt. 3).
   2) Wykonawca, w ramach aneksu, o którym mowa w pkt 1) powyżej, dostarczy wnioskowane Rozwiązanie w terminie do drugiego dnia kalendarzowego miesiąca następującego po dniu zawarciu umowy o udzielenie zamówienia publicznego z Zamawiającym.
   3) Szczegółowy wykaz pakietów został opisany w tabeli poniżej:

P/N	Nazwa produktu	Sposób licencjonowania	Okres obowiązywania	Ilość pakietów (miesięcznie*)
6QK-00001	Azure Monetary Commit ShrdSrvr ALNG subsVL MVL Commit (lub równoważne)	Pakiet/1 m-c	36 mies.	9

**oferta powinna zawierać koszt 9 pakietów pomnożonych przez cały okres Umowy (36 mies.)*

2. W przypadku zaoferowania rozwiązania równoważnego, Wykonawca może pominąć lub zmodyfikować podział na etapy, o którym mowa w ust. 1 pkt 1) i 2), jak również zmodyfikować ilość wskazanych powyżej pakietów oraz sposób ich licencjonowania, o ile dostawa rozwiązania równoważnego tego wymaga, z zastrzeżeniem osiągnięcia funkcjonalności opisanych w tabeli produktów.
3. Zamawiający wymaga, aby przedmiot zamówienia był świadczony przez Wykonawcę, który posiada najwyższy status partnerstwa przyznawany przez producenta oprogramowania, uprawniający do dostawy pakietów i objęcia ich pełnym wsparciem producenta przez cały okres trwania umowy. W przypadku zaoferowania usług równoważnych do usług Microsoft Azure posiada autoryzację producenta do sprzedaży i świadczenia usług tego rozwiązania;
4. Zamawiający wymaga dostawy rozwiązania w ramach polityki przewidzianej przez producenta oprogramowania, dla jednostek realizujących zadania publiczne;

5. Zasady dostawy rozwiązania:
   5.1. Zarządzanie pakietami subskrypcyjnymi realizowane będzie za pośrednictwem dedykowanego Portalu dostępowego producenta oraz konta Zamawiającego założonego w nim na adres licencje@coi.gov.pl;
   5.2. Zamawiający zostanie uprawniony w ramach posiadanych pakietów pakietów/licencji subskrypcyjnych do pobierania poprawek, aktualizacji i nowych wersji oprogramowania do końca obowiązywania subskrypcji w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego oprogramowania;
   5.3. Za pośrednictwem Portalu dostępowego[1] będą udostępniane dla oprogramowania:
      5.3.1. aktualne wersje, wydania uzupełniające, poprawki programistyczne, a także nowe wydania oprogramowania, będące kontynuacją linii produktowej;
      5.3.2. aktualizacje funkcjonalne i wspierające dla oprogramowania oraz poprawek bezpieczeństwa;
      5.3.3. nowe wersje oprogramowania obejmujące m.in. poprawki serwisowe, wersje wyższe (upgrade), wersje niższe (downgrade), wydania uzupełniające oraz poprawki oprogramowania wybranych wersji produktów;
      5.3.4. pliki instalacyjne dla oprogramowania w aktualnej i poprzednio wydanych przez producenta wersjach, niezwłocznie po ich udostępnieniu przez producenta oprogramowania;
   5.4. Zamawiający otrzyma dostęp za pośrednictwem Portalu dostępowego do aktualnej dokumentacji technicznej publikowanej i udostępnianej przez producenta oprogramowania;
   5.5. Zamawiający wymaga aby pakiety/licencje zostały dostarczone, tj. dodane do konta na Portalu dostępowym niezwłocznie po zawarciu Umowy, ale nie później niż w terminie do drugiego dnia kalendarzowego miesiąca następującego po dniu zawarciu umowy o udzielenie zamówienia publicznego z Zamawiającym ;
   5.6. Podstawą do odebrania przez Zamawiającego przedmiotu zamówienia jest dostarczenie na adres e-mail licencje@coi.gov.pl dokumentów potwierdzających dostarczenie rozwiązania, zawierającego co najmniej: numer umowy z producentem, numer klienta, pełną nazwę produktu, numer P/N produktu oraz liczbę pakietów/licencji. Potwierdzeniem odbioru przedmiotu zamówienia będzie protokół odbioru, podpisany obustronnie bez zastrzeżeń;
   5.7. Na wezwanie Zamawiającego Wykonawca dostarczy dokumenty potwierdzające status partnerstwa producenta rozwiązania;
6. Zgodność z obowiązującym prawem Polskim i Unijnym:
   6.1. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów członkowskich Unii Europejskiej;

[1] *Portal dostępowy – ujednolicona konsola oparta na sieci Web, umożliwiająca zarządzanie subskrypcjami, kontami użytkowników oraz tworzenie i monitorowanie zasobów.*

6.2. 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);
6.3. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego;
6.4. Gwarancja braku dostępu do danych Zamawiającego w usłudze, z wyłączeniem działań serwisowych wykonywanych wyłącznie przez uprawnione osoby z organizacji Dostawcy usługi;
6.5. Gwarancja usunięcia danych w terminie do 180 dni od wygaśnięcia subskrypcji i zakończenia umowy;

7. Pozostałe zasady realizacji niniejszego Zamówienia określone zostały w rozdziale III SIWZ Projektowane Postanowienia Umowy;
8. Przedmiot zamówienia jest refinansowany przez Skarb Państwa;

IV. Opis parametrów dla rozwiązania równoważnego

1. Zamawiający wskazuje, że zgodnie z przepisem art. 99 ust. 5 PZP dokonał opisu przedmiotu zamówienia poprzez wskazanie produktu referencyjnego oraz określenie poniższych parametrów równoważności;
2. Zamawiający dopuszcza jako „rozwiązanie równoważne" rozwiązanie zapewniające, bez dodatkowych nakładów finansowych (zgodnie ze złożoną Ofertą), bezkonfliktowe działanie posiadanego środowiska zbudowanego w oparciu o posiadane przez Zamawiającego licencje/pakiety subskrypcyjne, wskazane w *„Ogólnych warunkach realizacji Przedmiotu Zamówienia*". W przypadku dostarczenia rozwiązania równoważnego Wykonawca zapewni Zamawiającemu lub wskazanemu przez niego podmiotowi wykonanie implementacji tegoż rozwiązania w posiadanym przez Zamawiającego środowisku. W przypadku błędnego działania środowiska po wdrożeniu rozwiązania, Wykonawca będzie zobowiązany na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku takiej możliwości, do stanu pierwotnego, a także do dostarczenia innego rozwiązania spełniającego wymagania opisane poniżej;
3. Dostarczone rozwiązanie równoważne nie może w żaden sposób ograniczać obecnych funkcjonalności technicznych i dostępowych środowiska;
4. W przypadku zaoferowania przez Wykonawcę produktów równoważnych w stosunku do usług opisanych przez Zamawiającego wymagane jest, aby usługi spełniały niżej wymienione wymagania:
   4.1. Możliwość implementacji oprogramowania uruchomionego na istniejących konfiguracjach środowiska produkcyjnego i testowego Microsoft Azure;
   4.2. Zapewnienie całościowej migracji obecnego rozwiązania do rozwiązania równoważnego, w tym zapewnienie na czas migracji wsparcia posiadanych usług Microsoft Azure;
   4.3. Możliwość oddzielenia baz danych od serwerów aplikacyjnych przy czasie odpowiedzi nie przekraczającym 3 ms;
   4.4. Zapewnienie na czas migracji wspólnej infrastruktury autoryzacyjnej dla obu platform;

4.5. Rozwiązanie musi posiadać mechanizmy pozwalające na realizację wymagań rozliczalności i monitorowania użytkowników i usług;
4.6. Zapewnienie warunków i zakresu usługi wsparcia producenta dla produktów równoważnych nie gorszych niż opisane wymagania dla wsparcia technicznego obecnego producenta;
4.7. Zapewnienie warunków i zakresu usług asysty technicznej i konserwacji dla produktów równoważnych nie są gorszych, niż usługi oferowane przez obecnego producenta;

Platforma usług hostowanych

1. Subskrypcje platformy usług hostowanych:

Subskrypcja 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. Pula zasobów zakupionych w pakiecie musi umożliwić wykorzystanie:

1.1. Minimum 1 jednostki obliczeniowej o parametrach - 1 rdzeń procesora, 1,7 GB RAM, pod kontrolą systemu operacyjnego Windows Server lub Linux (wybrane dystrybucje);
1.2. Minimum 50 GB dostępnej lokalnie redundantnej przestrzeni dyskowej;
1.3. Minimum 50 GB dostępnej georedundantnej przestrzeni dyskowej (odległości min. 100km między lokalizacjami);
1.4. Minimum 100 GB transferu danych do i z usługi miesięcznie;

2. Dostępny portal administracyjny, pozwalający na uruchamianie poprzez wybór dostępnych usług;
3. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci);
4. Możliwość wyboru różnych rodzajów dysków i ich pojemności;
5. Zarządzanie za pomocą graficznego interfejsu użytkownika oraz skryptów, z możliwością zdalnego dostępu;
6. Komunikacja z mechanizmami zarządzania usługi poprzez REST API;
7. Możliwość przechowywania danych spełniająca następujące wymagania (opcjonalnie dostępnych w ramach usługi):
   7.1 Wysoka skalowalność, auto-partycjonowanie, load-balancing;
   7.2 Obsługa przechowywania danych udostępnianych jako blob, tablica, dysk, plik, kolejka;
   7.3 Wsparcie dla systemów klienckich Windows i Linux;
   7.4 Skalowalność pojedynczego zasobu pamięci 500TB;
   7.5 Replikacja danych - min. 3 kopie w ramach pojedynczej lokalizacji;
   7.6 Replikacja do innej lokalizacji oddalonej o min 100km od lokalizacji podstawowej;
   7.7 Udostępnienie zasobów pamięci poprzez REST API;
   7.8 Gotowe biblioteki programistyczne środowisk programowania: .NET, Java/Android, Node.js, PHP, Ruby, Python, PowerShell;
8. Konfigurowalne usługi wyszukiwania treści w zasobach własnych i Internet;
9. Konfigurowalne usługi analizy wyszukanych treści;
10. Dostępność usług umożliwiających uruchamianie aplikacji WWW w modelu gotowej do wykorzystania usługi, z utrzymywanymi 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;

11. 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;
12. Dostępność relacyjnej i nierelacyjnej bazy danych, w tym oparte o technologię Hadoop, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%;
13. 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%. WZ/06/2022 13. 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;
14. Dostępny portal administracyjny, pozwalający na uruchamianie usług poprzez wybór spośród dostępnych usług;
15. Możliwość powoływania maszyn wirtualnych poprzez wybór z gotowych szablonów zawierających różne ich konfiguracje (liczbę rdzeni, pamięci);
16. Włączenie reguł wymuszających stosowanie się do odpowiedniej nomenklatury nazewnictwa zasobów w obrębie środowiska, wymuszając wykorzystanie ustalonego modelu nazw, prefiksów dla określonych typów zasobów;
17. Dostępność usług umożliwiających utworzenie prywatnego repozytorium obrazów kontenerów w standardzie zgodnym z Docker;
18. 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
19. Dostępność relacyjnych baz danych, zgodnych z MySQL i z PostgreSQL, dostępnych jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%;
20. Dostępność bazy danych typu NoSQL, oferującej API dostępowe zgodne z MongoDB dostępnej jako gotowe do wykorzystania usługi o poziomie dostępności minimum 99,9%;
21. Przynajmniej dwa jasno zdefiniowane poziomy spójności danych dla bazy NoSQL;
22. Możliwość automatycznej dystrybucji danych pomiędzy różne regiony oraz ulokowane w nich centra obliczeniowe wraz z możliwością ręcznego jak i automatycznego przełączania replik;
23. Możliwość zestawienia dedykowanego łącza pomiędzy siedzibą Zamawiającego a dostawcą usług chmurowych w technologii opartej o światłowody;
24. Posiadanie przez dostawce centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających cykliczne raporty na temat aktualnych zagrożeń i sposobie ich zwalczania;
25. Akcelerowana, definiowana programowo sieć wirtualna w środowisku, wspierająca akcelerację SR-IOV, realizowana na akcelerowanych interfejsach sieciowych FPGA, do 30Gb/s.
26. Możliwość śledzenia ruchu sieciowego;

27. 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;
28. Możliwość wykorzystania usług SMB 3.0 do współdzielenia plików wykorzystując szyfrowanie podczas transmisji, jako usługa;
29. Możliwość zdefiniowania szablonu maszyny wirtualnej włącznie z konfiguracją aplikacji, uruchamiania serwisów poprzez zdefiniowanie stanu oczekiwanego w postaci plików konfiguracyjnych;
30. 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 usług z możliwością ich okresowego wyłączania;

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 niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi;
7. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory;
8. Dostępność mechanizmu uwierzytelnienia wieloskładnikowego;
9. 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”;
10. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych;
11. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN);
12. Wbudowane mechanizmy zabezpieczające przez atakami DDoS;
13. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 500 km, znajdujące się na terenie Unii Europejskiej;
14. Silnik rekomendacji zabezpieczeń infrastruktury oparty o algorytmy nauczania maszynowego;
15. Dostępność usługi umożliwiającej przechowywanie certyfikatów, haseł dostępu zgodnie ze standardem FIPS 140-2 poziomu 2;

16. 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);
17. Dostępność usługi katalogu tożsamości i przynależności użytkowników do grup wspierający OAuth2 oraz pojedynczego logowania, umożliwiający budowanie logowania przy pomocy dostawców firm trzecich;
18. Oba centra danych powinny posiadać przynajmniej trzy z wymienionych certyfikacji: **TIER-III** lub równoważny, **UK G-Cloud** lub równoważny, **ENISA IAF** lub równoważny, **SOC 1** lub równoważny, **SOC 2** lub równoważny;
19. Zamawiający wymaga dostępności następujących mechanizmów bezpieczeństwa w ramach usługi:
    19.1. Bramki VPN;
    19.2. Obsługi IPSec;
    19.3. Akceleracji SSL;
    19.4. Firewalla warstwy aplikacyjnej (WAF);
    19.5. Load balancera wspierającego Cookie Affinity;
    19.6. Systemu przeciwdziałania włamaniom – IPS;
    19.7. Systemu wykrywania włamań – IDS
    19.8. Zasobów ludzkich w zakresie utrzymania usługi realizacji zadania prewencji, identyfikacji zagrożeń oraz natychmiastowe reagowanie na wszelkie incydenty bezpieczeństwa IT;
    19.9. Posiadanie przez dostawce centrów przetwarzania, działających w trybie 24/7 zespołów monitorujących i zwalczających cyberataki oraz przedstawiających raporty na temat aktualnych zagrożeń i sposobie ich zwalczania;
20. Wymagane jest zapewnienie dostępności platformy i jej bezpieczeństwo poprzez:
    20.1. Zagwarantowanie poziomu dostępności na poziomie minimum 99,9%;
    20.2. Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm;
    20.3. 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;
    20.4. Możliwość skalowania usługi z przewidywalnymi kosztami takiego skalowania;
    20.5. Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi;
    20.6. Możliwość wdrażania nowej wersji aplikacji bez przestoju w pracy dotychczasowego środowiska;
    20.7. Dostępność mechanizmów monitorowania zachowania użytkowników usługi oraz prób Dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego;
    20.8. Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej;
    20.9. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory;

20.10. 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”;
20.11. Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych;
20.12. Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN);
20.13. Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS;
20.14. Przynajmniej dwa równorzędne ośrodki przetwarzania danych, odległe od siebie o co najmniej 100 km;
20.15. Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Europejskiego Obszaru Gospodarczego;
20.16. Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/ składowanych w usłudze danych po stronie Zamawiającego;
20.17. Gwarancję usunięcia danych Zamawiającego z Platformy po zakończeniu umowy;
20.18. Gwarancję braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody Zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy Platformy;
20.19. Zapewnienie wsparcia Platformy dla standardowych rozwiązań OpenSource takich jak Tomcat, SugarCRM, ownCloud, Redmine, MediaWiki, LimeSurvey, Moodle czy Liferay. Dostępność w ramach platformy predefiniowanych obrazów z tym oprogramowaniem;

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:
   2.1. **ISO 27001** lub równoważny, **ISO 27002** lub równoważny, **ISO 27017** lub równoważny, **ISO 27018** lub równoważny, **SOC 1** lub równoważny, **SOC 2** lub równoważny, **SOC 3** lub równoważny, **Open Authentication Standard** lub równoważny, **Oauth** lub równoważny;
   2.2. W zakresie interoperacyjności:
      2.2.1. HTTP(S);
      2.2.2. TLS;
      2.2.3. Docker;
      2.2.4. REST API;
   2.3. W zakresie programowania:
      2.3.1. Java;
      2.3.2. NET;
      2.3.3. PHP;
      2.3.4. Python;

2.3.5. Node.js;
2.3.6. Wsparcie narzędziowe w Visual Studio i Eclipse;

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

Wymagania dotyczące dostawy rozwiązania równoważnego

1. Tam, gdzie Zamawiający opisał przedmiot zamówienia za pomocą norm, certyfikatów zgodnie z art. 101 ust. 4 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym. Zgodnie z art. 101 ust. 5 ustawy Pzp, Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, zobowiązany jest udowodnić w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 ustawy Pzp, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia lub wykazać powyższą równoważność poprzez złożenie wraz z ofertą *„Wykazu parametrów oferowanych lub opis sposobu spełniania wymagań zawartych w OPZ”* stanowiącego załącznik nr 5 do Formularza oferty na potwierdzenie że:
   a) wykonawca dostarczy przedmiot zamówienia, który posiada certyfikat lub spełnia równoważne wymagania certyfikatu zgodności z **ISO 27001**, **ISO 27002**, **ISO 27017**, **ISO 27018**, **SOC 1**, **SOC 2**, **SOC 3**, **Open Authentication Standard**, **Oauth** w pkt. 58.1, 58.2, 58.3, 58.4, 58.5, 58.6, 58.7, 58.8, 58.9 poprzez zaznaczenie - ☐ “SPEŁNIA”;
   b) wykonawca dostarczy przedmiot zamówienia, który posiada certyfikat lub spełnia równoważne wymagania certyfikatu zgodności obu centrów danych posiadających przynajmniej trzy z wymienionych certyfikacji: **TIER-III**, **UK G-Cloud**, **ENISA IAF**, **SOC 1**, **SOC 2** w pkt. 54 poprzez zaznaczenie- ☐“SPEŁNIA”.