Załącznik nr 2 do SIWZ

**Szczegółowy opis przedmiotu zamówienia.**

W niniejszym załączniku przedstawiono minimalne wymagania i parametry usług w chmurze dla wdrożenia Platformy Integracyjnej.

1. **POSTAWOWE WYMAGANIA I PARAMETRY INFRASTRUKTURY**
   1. **IaaS**

W obszarze dostawy zasobów infrastrukturalnych (IaaS), oprócz udostępnianej mocy obliczeniowej, zostaną uruchomione również usługi IT obejmujące:

* + 1. **Podsystem monitorowania i zdalnego dostępu do IaaS i PaaS.**

1. w ramach IaaS musi zostać udostępniony interfejs, który po przeprowadzeniu uwierzytelnienia i autoryzacji umożliwi zdalny dostęp do komponentów chmurowych,
2. udostępniony interfejs musi umożliwiać instalowanie oprogramowania systemowego, aplikacji, monitorowanie dostępności komponentów chmurowych oraz ich wydajności,
3. monitoring będzie udostępniał widoki on-line kluczowych metryk i alertów infrastruktury.

**1.1.2. Podsystem backupu**

1. usługa obejmie implementację polityki wykonywania kopii bezpieczeństwa,
2. usługa obejmie dane Systemu Platformy Integracyjnej w obu ośrodkach: CPD i ZCPD,
3. usługa powinna umożliwiać odtworzenie Systemu PI do wybranego punktu w czasie,
4. rozwiązanie musi umożliwiać testowe odtwarzanie kopii bezpieczeństwa w trakcie normalnej pracy,
5. zakładane parametry czasowe dla scenariusza Disaster Recovery (DR), bazującego na odtworzeniu środowiska produkcyjnego z backupów, wynoszą: RPO = 24 h , RTO = 8 h,
6. wstępne założenia do określenia wolumetrii retencji składowanych danych: 30/31 pełnych kopii dziennych z bieżącego miesiąca, pełne kopie tygodniowe z miesiąca poprzedzającego, 10 pełnych kopii na żądanie,
7. pełna integracja z platformą wirtualizacyjną, kopie maszyn wirtualnych wykorzystujące mechanizm snapshoot.

**1.1.3. Raportowanie parametrów SLA.**

1. czas niedostępności będzie liczony z dokładnością do 1 minuty,
2. niedostępności krótsze niż 1 min będą notyfikowane w podsystemie monitorowania,
3. raporty dostępności będą dotyczyły wszystkich usług (VM, Monitoring, VPN, Backup, DR, Bezpieczeństwo) świadczonych w obszarze dostawy IaaS.
   * 1. **Usługę przełączenia przetwarzania produkcyjnego w przypadku awarii CPD.**
4. wydajność ośrodka zapasowego (ZCPD) powinna być równa wydajności CPD tzn. zasoby oraz komunikacja z ZCPD powinny być zapewnione w taki sposób, aby po przełączeniu na ośrodek zapasowy w systemie nie był odczuwalny spadek wydajności do czasu ponownego przełączania na ośrodek podstawowy,
5. rozwiązanie musi umożliwiać testowanie przełączenia środowiska produkcyjnego w trakcie normalnej pracy,
6. replikowanie asynchroniczne do ZCPD wszystkich danych tworzonych i składowanych w CPD,
7. replikowanie asynchroniczne do CPD wszystkich danych produkcyjnych składowanych w ZCPD,
8. zakładane parametry czasowe w scenariuszu DR (Disaster Recovery) to RPO 15 min,

RTO 1 h.

* + 1. **Bezpieczeństwo**

1. usługa implementuje mechanizmy ochrony przed nieuprawnionym dostępem, szkodliwym oprogramowaniem i atakami z Internetu,
2. usługa udostępnia notyfikacje bezpieczeństwa, alarmy i raporty podatności.
   * 1. **Zapewnienie możliwości kolokacji sprzętu lub oprogramowania z serwerowniami ZTM (w przypadku posadowienia w nich funkcjonalności wspierającej system Platformy Integracyjnej) w zakresie:**
3. zapewnienia retencji danych,
4. monitorowania i zarządzania wydajnością aplikacji,
5. zarządzania użytkownikami i/lub kluczami kryptograficznymi,
6. zarządzania konfiguracją lub instalacją.
   1. **PaaS**
      1. W obszarze dostawy PaaS Zamawiający zakłada:
7. zapewnienie środowiska uruchomieniowego Docker na potrzeby instalacji oprogramowania funkcjonalnego Platformy Integracyjnej,
8. zapewnienie możliwości dostarczenia oprogramowania na środowisko produkcyjne w postaci obrazów Docker (utrzymywania lokalnego rejestru obrazów),
9. zapewnienie instancji bazodanowych PostgreSQL pracujących w modelu HA,
10. deployment rozwiązania w klastrze niezawodnościowym.
11. **ZAKŁADANY PROGRAMOWY STOS TECHNOLOGICZNY DLA ŚRODOWISKA PRODUKCYJNEGO**
    1. Zdefiniowany stos technologiczny Platformy Integracyjnej wynikający, z potrzeby zachowania zgodności z technologiami aktualnie stosowanymi przez Zamawiającego (wirtualizacja, backup), oraz wymagań konstrukcyjnych i wdrożeniowych budowanego oprogramowania Platformy Integracyjnej.
       1. Wirtualizacja - VMware 6.5 Enterprise Plus (vSphere i vCenter Server).
       2. System backup - Veeam Backup & Replication.
       3. System operacyjny (Windows) zapewniający wsparcie dla systemu backupu Veeam.
       4. System operacyjny klasy Linux zapewniający wsparcie dla sklastrowanej konteneryzacji Docker.
       5. Lokalna baza danych - PostgreSQL 10.
       6. Zarządzanie klastrem PostgreSQL – PgPool.
       7. Konteneryzacja - Docker CE 17.12.1 (w modelu Swarm).
       8. System zarządzania konteneryzacją - Portainer 1.18.1.
       9. LDAP Platformy Integracyjnej - Apache Directory Studio.
       10. Zarządzanie logami - Logstash/ElasticSearch/Kibana.
       11. Zarządzanie komunikatami danych – RabbitMQ.
       12. Framework programistyczny - Java Spring Boot 2.
       13. Serwer aplikacyjny - Tomcat 8.5.
       14. Software loadbalancer - Nginx 1.15.
       15. Edge gateway - Nginx 1.15.
       16. Application gateways - Netflix Zuul 2.x.
       17. Rejestr usług i zarządzanie konfiguracją – Consul.
       18. Automatyzacja zadań IT – Ansible.
12. **SZCZEGÓŁOWE WYMAGANIA I PARAMETRY INFRASTRUKTURY**
    1. **WYMAGANIA MINIMALNE DOTYCZACE INFRASTRUKTURY CPD**
       1. Zasoby serwerowe dedykowanej chmury prywatnej ośrodka podstawowego, muszą być zarezerwowane wyłącznie dla obsługi Platformy Integracyjnej.
       2. Zasoby powinny być umieszczone w data center spełniającym wymogi co najmniej TIER III.
       3. Serwery CPD zostaną umieszczone w strefie bezpieczeństwa data center odpowiadającej przepisom   
          o ochronie danych osobowych (wg RODO). System monitoringu zapewni zdalny dostęp dla administratorów systemu Platformy Integracyjnej.
       4. CPD musi być połączone łączem światłowodowym o przepustowości przynajmniej 10Gbps z serwerownią produkcyjnego systemu ŚKUP Zamawiającego w lokalizacji: Katowice ul. Barbary 21a.
       5. CPD i ZCPD musi zapewnić połączenie do internetu bez limitu danych i bez limitu możliwych do zdefiniowania zewnętrznych adresów IP oraz z możliwością szybkiego przeniesienia adresacji między ośrodkami.
       6. CPD musi zapewniać możliwość ustawiania połączeń VPN.
       7. Połączenie do internetu musi być zabezpieczone rozwiązaniem firewall (Firewall New Generation with IPS) pracującym w modelu HA active/active. Połączenia z serwerami Platformy Integracyjnej muszą być zabezpieczone firewall-em aplikacyjnym (WAF).
    2. **WYMAGANIA MINIMALNE DOTYCZACE INFRASTRUKTURY ZCPD**
       1. Zapasowy ośrodek przetwarzania (ZCPD), Wykonawca zbuduje w oparciu o chmurowe zasoby współdzielone.
       2. ZCPD powinno być zbudowane w innej lokalizacji niż CPD.
       3. System monitoringu powinien umożliwiać zdalny dostęp dla administratorów systemu Platformy Integracyjnej.
       4. ZCPD musi zapewniać możliwość ustawiania połączeń VPN.
       5. Połączenie do internetu musi być zabezpieczone w sposób zapewniający analogiczny poziom bezpieczeństwa, jak połączenie do internetu w CPD.
    3. **WYMAGANIA MINIMALNE DOTYCZACE URZĄDZEŃ HSM**
       1. W ramach środowiska produkcyjnego Platformy Integracyjnej Wykonawca zapewni w obszarze usługi IaaS lub PaaS urządzenia HSM do przechowywania kluczy kryptograficznych dla środowiska produkcyjnego Platformy Integracyjnej. Usługa umożliwi pełną konfigurację, administrację i użytkowanie urządzenia HSM kolokowanego z chmurowym środowiskiem produkcyjnym Platformy Integracyjnej przez okres jednego roku od uruchomienia środowiska.
       2. Możliwość wykonania przynajmniej następujących operacji:

a. generowanie par kluczy kryptograficznych,

b. fizyczna i logiczna ochrona kluczy kryptograficznym,

c. kontrola dostępu do kluczy kryptograficznych,

d. wykonywanie operacji z użyciem kluczy kryptograficznych,

e. archiwizacja kluczy,

f. odtwarzanie kluczy po awarii urządzenia.

* + 1. Możliwość generowania kluczy dla algorytmu RSA o różnej sile: klucze 1024 bity, 2048 bitów oraz 4096 bitów.
    2. Możliwość montażu w szafie 19” z dostarczonymi w komplecie odpowiednimi uchwytami.
    3. Urządzenie musi posiadać minimum 2 interfejsy Ethernet 100 Mbit/s.
    4. Urządzenie musi pozwalać na archiwizację kluczy i ich odtwarzanie w przypadku uszkodzenia urządzenia. Archiwizacja kluczy musi wykorzystywać mechanizm podziału sekretu.
    5. Urządzenie musi być dostarczone wraz z niezbędnymi komponentami i nośnikami służącymi do archiwizacji kluczy, umożliwiającymi pełne wykonanie kopii zapasowych materiału kryptograficznego i pełne odtworzenie materiału kryptograficznego.
    6. Urządzenie musi mieć pojemność min. 100 kluczy kryptograficznych RSA 2048 oraz możliwość tworzenia slotów. Możliwość zarządzania urządzeniem z poziomu linii poleceń jak i interfejsu graficznego.
    7. Urządzenie musi wspierać podłączenie do wirtualizatora VMWare (ESXi).
    8. Urządzenie musi zapewniać prędkość wykonywania operacji kryptograficznych z użyciem algorytmu RSA z kluczem o długości 2048 bity min. 16 operacji na sekundę lub większą.
    9. Urządzenie powinno umożliwiać przetrzymywanie kluczy kryptograficznych wewnątrz modułu HSM.
    10. Urządzenie musi być zgodne z wymaganiami RoHS.
    11. Urządzenie musi wspierać systemy operacyjne: Windows Server 2012, Windows Server 2012R2, oraz nowsze, Linux.
    12. Urządzenie powinno wykorzystywać moduł kryptograficzny posiadający poziom bezpieczeństwa FIPS 140-2 Level 3 potwierdzony wydanym dla tego modelu urządzenia certyfikatem.
    13. Urządzenie musi być wyposażone w dwa zasilacze.
    14. Urządzenie musi być dostarczone z oświadczeniem potwierdzającym nienaruszenie urządzenia od momentu opuszczenia zakładu producenta.
    15. Urządzenie nie może ograniczać ilości połączeń do HSM (poza wydajnością urządzenia).
    16. Urządzenie nie może ograniczać ilości klientów lub aplikacji podłączających się do urządzenia.
    17. Urządzenie nie może mieć ograniczeń przy zdalnej administracji urządzeń.
    18. Urządzenie musi wspierać interfejsy programistyczne (API): PKCS#11, Java Cryptography Extension (JCE), Microsoft Crypto API (CSP), Cryptography Next Generation (CNG) and SQL Extensible Key Management (SQLEKM).
    19. Urządzenie musi wspierać algorytmy: RSA, DSA, ECDSA with NIST and Brainpool curves, DH, ECDH with NIST and Brainpool curves, AES, Triple-DES, DES, MAC, CMAC, HMAC, SHA-1, SHA2-Family, SHA3, RIPEMD, True Random Number Generator (TRNG acc. AIS31 class PTG.2).
    20. Urządzenie musi mieć poświadczoną zgodność z normami: FIPS 140-2 Level 3\*, CE, FCC Class B, UL, IEC/EN 60950-1, CB certificate, RoHS II, WEEE.
    21. Wymagane wsparcie i gwarancja producenta nie krótsze niż 12 miesięcy.
    22. Wraz z urządzeniem należy dostarczyć czytnik PIN (PINPad reader) dedykowany do urządzenia, oraz 10 kart inteligentnych współpracujących z urządzeniem.
  1. **MINIMALNE WYMAGANIA WOLUMETRYCZNE**
     1. W ramach usługi udostępniania zasobów (IaaS) dla CPD powinien być zapewniony, we wskazanych poniżej punktach czasowych:
     2. **ETAP 1.** W momencie uruchomienia środowiska, gwarantowany dostęp do:
     3. mocy obliczeniowej min 27 vCPU,
     4. pamięci operacyjnej min 140 GB (vRAM),
     5. wirtualnej przestrzeni dyskowej w CPD minimum o pojemności 1,4 TiB i przepustowości 1000 IOPS,
     6. **ETAP 2.** Od „punktu zwiększenia”, gwarantowany dostęp do:
     7. mocy obliczeniowej min 39 vCPU,
     8. pamięci operacyjnej min 268 GB (vRAM),
     9. wirtualnej przestrzeni dyskowej w CPD minimum o pojemności 2,7 TiB i przepustowości 1000 IOPS,
     10. Dla każdego etapu Wykonawca zapewni odpowiednią pojemność na kopie bezpieczeństwa, replikację oraz przełączanie ośrodków.
     11. Przez „punkt zwiększenia” Zamawiający rozumie datę, w której zakłada się zwiększenie zasobów zapewnianych przez środowisko. Data zostanie ustalona pomiędzy Wykonawcą a Zamawiającym na koniec czerwca 2019 i będzie się zawierać w przedziale od 1.08.2019 do 1.11.2019.
     12. W ramach CPD Wykonawca zapewni środowisko wysokiej dostępności (HA) zbudowane bez pojedynczego punktu awarii sprzętowej które odpowiadać będzie specyfikacji konfiguracyjnej:
     13. Warstwa wirtualizacyjna zostanie wykonana z wykorzystaniem oprogramowania VMware vSphere 6.5 lub wyższym.
     14. Zasoby CPU/RAM powinny zostać zapewnione przez zestaw co najmniej 2 serwerów fizycznych.
     15. Wszystkie powołane (w ilości 10 do 22) maszyny wirtualne oraz dane będą przechowywane na macierzowych zasobach dyskowych.
     16. Na powołanych maszynach wirtualnych powinny zostać zainstalowane systemy operacyjne klasy Linux, zapewniających obsługę sklastrowanego środowiska konteneryzacji Docker.
     17. W ramach dostawy zasobów Wykonawca zapewni środowisko wysokiej dostępności dla zasobów software’owych w oparciu o systemowe rozwiązania klastrowe gdzie na poziomie maszyn wirtualnych (VM), zostanie wykorzystany mechanizm Failover z pakietu oprogramowania Vmware vSphere HA (IaaS).
  2. **MINIMALNE WYMAGANIA WYDAJNOŚCIOWE**
     1. Moc obliczeniowa serwerów zostanie przygotowana przez Wykonawcę tak by spełnić następujące wymagania wydajnościowe:
     2. Serwery fizyczne udostępniające zasoby IaaS będą wykorzystywały procesory firmy Intel o częstotliwości taktowania nie mniejszej niż 2,2 Ghz i wyniku testu CPU2017 Integer Rate Base na poziomie przynajmniej 90 (opublikowany na stronie www.spec.org) lub inne procesory zapewniające analogiczną lub wyższą wydajność.
     3. Przepustowość kanałów dyskowych do wolumenów dyskowych utworzonych na macierzach wyniesie co najmniej 1 000 IOPS (read/write operations - 50/50).
     4. Interfejsy Ethernet serwerów fizycznych powinny pracować z prędkością 10Gbps.
     5. Pasmo przepustowości łącza CPD z dostawcą Internetu powinno pracować z prędkością minimum 0,5 Gbps.
     6. Pasmo przepustowości łącza CPD z serwerownią Zamawiającego powinno pracować z prędkością 10 Gbps.
     7. Połączenie VPN, udostępniane z CPD /ZCPD powinno charakteryzować się pasmem przepustowości nie mniejszym niż 64kbps.
  3. **MINIMALNE ZAŁOŻENIA DOTYCZĄCE USŁUGI UDOSTĘPNIANIA ZASOBÓW**
     1. Usługa powinna zapewniać udostępnianie zasobów co najmniej do marca 2021 włącznie.
     2. Fizyczna lokalizacja Centrów Danych musi się znajdować na terenie Europejskiego Obszaru Gospodarczego.
     3. Usługa powinna zapewniać możliwość uzgodnienia zwiększenia gwarantowanej mocy przetwarzania oraz wielkości i wydajności zasobów dyskowych na przełomie lat 2019/2020 i połowie 2020, w związku   
        z rozwojem funkcjonalnym Systemu.
     4. Usługa konfiguracji i udostępniania usług chmurowych zapewniać będzie:
        + 1. Zorganizowanie i pokrycie kosztów wymaganej infrastruktury IT.
          2. Pokrycie kosztów kolokacji oraz publicznej adresacji IP dla środowiska IT.
          3. Pokrycie kosztów energii elektrycznej .
          4. Ciągłe monitorowanie parametrów fizycznych w serwerowni (klimatyzacja, zasilanie, wilgotność, temperatura).
          5. Ciągły monitoring infrastruktury serwerowej, macierzowej oraz urządzeń sieciowych, a także środowiska wirtualizacyjnego i systemów operacyjnych w nim posadowionych.
          6. Zarządzanie (w tym procedury naprawcze) infrastrukturą serwerową, macierzową i sieciową (bez limitu roboczogodzin).
          7. Odpowiednie prawa licencyjne lub sublicencyjne do korzystania z usługi i zapewnienie wsparcia dla oprogramowania Vmware vSphere i vCenter Server, system backupu, systemów operacyjnych dla systemu backupu, systemów operacyjnych klasy Linux, baz danych klasy PostgreSQL oraz zarządzania wydajnością aplikacji i monitoringu systemu jeśli są wymagane
          8. Monitoring środowiska wirtualizacyjnego (bez limitu roboczogodzin).
          9. Zarządzanie środowiskiem wirtualizacyjnym, maszynami wirtualnymi i systemami operacyjnymi   
             (z limitem wprowadzania zmian w konfiguracji na poziomie przynajmniej 32 roboczogodzin miesięcznie).
          10. Zarządzanie polityką, środowiskiem oraz zadaniami backupu i odtworzeniami (z limitem na poziomie przynajmniej 16 roboczogodzin miesięcznie)
          11. Pełną obsługę serwisowo-gwarancyjną
          12. Helpdesk dostawcy usług chmurowych w trybie 24/7/365
     5. Usługę zapewnienia środowisko pilota wykorzystania urządzeń HSM do przechowywania kluczy kryptograficznych
     6. Zapewnienie licencji maintenance dla każdego z wykorzystywanego oprogramowania infrastrukturalnego, dopuszcza się jednak model zapewniania ciągłości działania takiego oprogramowania bez wykupienia takich licencji, w oparciu o kompetencje ekspertów dostarczającego usługi chmurowe. W takim przypadku dopuszczalne jest obniżenie poziomu SLA dla wybranych elementów ITS.
     7. W ramach umowy dostarczania usług chmurowych Wykonawca udostępni skonfigurowane i gotowe do użycia środowisko zgodnie z wytycznymi Zamawiającego w tym:
        1. Kolokację sprzętu.
        2. Konfigurację środowiska wirtualizacji i maszyn wirtualnych zgodnie z przekazanymi wytycznymi przez Zamawiającego.
        3. Instalację i konfigurację systemów operacyjnych zgodnie z przekazanymi wytycznymi przez Zamawiającego.
        4. Konfigurację dostępów i konfigurację sieciową zgodnie z przekazanymi wytycznymi przez Zamawiającego.
        5. Konfigurację monitoringu zgodnie z przekazanymi wytycznymi przez Zamawiającego.
        6. Instalację i konfigurację systemu backupu zgodnie z przekazanymi wytycznymi przez Zamawiającego.
        7. Instalację i konfigurację silnika bazy danych zgodnie z przekazanymi wytycznymi przez Zamawiającego.
        8. Model dostępności usług w miesięcznym rozliczeniu abonamentowym.
        9. Rozliczenia usług w sposób uzależniony od realnego zużycia zasobów.
        10. SLA na poziomie 99,95% dostępności miesięcznej i rocznej.
        11. Możliwość skalowania poziomego i pionowego każdego z elementów infrastruktury (IaaS).
        12. Możliwość objęcia monitoringiem baz danych i środowiska konteneryzacji monitoringiem (PaaS).
  4. **MINIMALNE WYMAGANIA DOTYCZĄCE MOŻLIWOŚCI ROZBUDOWY**
     1. Moc obliczeniowa rozwiązania klastrowego (IaaS) powinna mieć możliwość powiększenia o 100%   
        w trybie ‘on-demand”.
     2. Pasmo przepustowości połączenia z internetem powinno mieć możliwość zwiększenia o 100% w trybie ‘on-demand’**.**