

OPIS PRZEDMIOTU ZAMÓWIENIA
do Wstępnych Konsultacji Rynkowych związanych z postępowaniem o udzielenie
zamówienia publicznego na modernizację infrastruktury teleinformatycznej
i rozbudowę funkcjonalności Systemu Informacji Przestrzennej Administracji Morskiej
(SIPAM)

I. Opis Systemu Informacji Przestrzennej Administracji Morskiej (SIPAM)

Centralnym punktem obecnego SIPAM jest relacyjno-objektowa baza danych (PostgreSQL¹ z rozszerzeniem PostGIS²) GIS³, która jest magazynem danych wektorowych oraz opisowych. Dostęp do danych następuje poprzez węzeł publiczny, który integruje dane pochodzące z węzłów lokalnych (węzeł lokalny Urzędu Morskiego w Gdyni, węzeł lokalny Urzędu Morskiego w Szczecinie, węzeł lokalny Ministerstwa Infrastruktury).

Głównym punktem dostępu do danych jest internetowa aplikacja mapowa Geoportal SIPAM, oparta o serwer danych przestrzennych Geoserver⁴. Geoportal SIPAM zawiera standardowe funkcjonalności związane z wizualizacją i analizą danych przestrzennych oraz zawiera narzędzia przeznaczone dla administracji morskiej. Geoportal SIPAM zawiera zestaw predefiniowanych kompozycji mapowych.

Udostępnienie danych w sieci Internet następuje poprzez użycie następujących standardów:

- Standardy Open Geospatial Consortium (OGC): WMS (Web Map Service), WFS (Web Feature Service), CS-W (Catalog Service for Web), ATOM
- Standardy użyte do budowy API: SOAP.

Baza danych zawiera ponad 34 zharmonizowane zbiory danych dostępne do tej pory jedynie w formie analogowej lub w formie niezharmonizowanej.

Rozmiar posiadanych danych wynosi ok. 15 TB. Obecnie jest udostępnionych online ponad 6 500 sztuk dokumentów zawierających informacje sektora publicznego.

Zamawiający posiada własną infrastrukturę teleinformatyczną zlokalizowaną w dwóch centrach przetwarzania danych w Urzędzie Morskim w Gdyni oraz Urzędzie Morskim w Szczecinie. Zamawiający dysponuje środowiskiem do wirtualizacji zasobów. Maszyny wirtualne umieszczone są w klastrze z zastosowaniem rozwiązań wysokiej dostępności. Dla systemu stosowane są mechanizmy równoważenia obciążenia. Obecnie infrastruktura teleinformatyczna jest objęta wsparciem technicznym, które kończy się w listopadzie 2027 r.

¹ <https://www.postgresql.org.pl/>

² <https://postgis.net/>

³ Geographic Information System

⁴ <https://geoserver.org/>

Szczegółowy zakres funkcjonalności oraz aspekty techniczne SIPAM zostały opisane w dokumentacji, która zostanie udostępniona uczestnikom wstępnych konsultacji rynkowych:

- Podręcznik użytkownika SIPAM,
- Schemat połączeń SIPAM,
- Dokumentacja bazy danych.

II. Planowany zakres zamówienia publicznego na modernizację infrastruktury teleinformatycznej i rozbudowę funkcjonalności Systemu Informacji Przestrzennej Administracji Morskiej (SIPAM2)

Zamawiający planuje zamówić następujące dostawy i usługi:

1. Wykonanie analizy przedwdrożeniowej,
2. Dostawa infrastruktury teleinformatycznej,
3. Dostawa i wdrożenie systemu informatycznego SIPAM2,
4. Migracja danych do SIPAM2,
5. Usługi serwisu gwarancyjnego oraz wsparcia technicznego dla SIPAM2.

Wyniki analizy przedwdrożeniowej, w tym rejestr wymagań, koncepcja rozwiązania, projekt architektury oraz plan migracji, wymagają akceptacji Zamawiającego i stanowią podstawę realizacji kolejnych etapów zamówienia.

1. Wykonanie analizy przedwdrożeniowej

Analiza przedwdrożeniowa będzie uwzględniała następujące aspekty:

- 1) Audyt istniejących procesów biznesowych w zakresie administracji morskiej wspieranych przez system SIPAM wraz z propozycją ich usprawnienia;
- 2) Audyt istniejącej funkcjonalności systemu SIPAM oraz ich ocena;
- 3) Od sierpnia 2026 r. rozpoczął funkcjonowanie Urząd Morski w Słupsku, który należy włączyć w proces gromadzenia i aktualizacji danych, analogicznie jak dla pozostałych urzędów;
- 4) Wyjściowy zakres funkcjonalności dla systemu SIPAM2 będzie co najmniej na poziomie funkcjonalności istniejącego systemu SIPAM;
- 5) Analiza istniejącej infrastruktury teleinformatycznej: weryfikacja sprzętu, sieci oraz oprogramowania systemowego;
- 6) Analiza pod kątem wymagań docelowej infrastruktury teleinformatycznej, tj. wdrożenia systemu SIPAM2 na zmodernizowanym sprzęcie zlokalizowanym w Urzędzie Morskim w Gdyni;
- 7) Analiza i zaprojektowanie sposobu wdrożenia nowych funkcjonalności:

- a. harmonizacja danych do schematów INSPIRE,
- b. utworzenie kreatorów wniosków m.in. o wydanie pozwoleń lokalizacyjnych w polskich obszarach morskich oraz wniosków o zgodę na wykorzystanie pasa technicznego,
- c. aktualizację wszystkich wersji komponentów SIPAM do najnowszych stabilnych wersji – jeżeli dotyczy;
- d. likwidację węzłów lokalnych mgm-local, umg-local i ums-local – dostęp do funkcjonalności SIPAM2 możliwy będzie z wykorzystywaniem węzła publicznego;
- e. zmiana modelu danych dla granicznej linii ochrony oraz minimalnych poziomów brzegu morskiego w celu dostosowania do możliwości prezentacji danych pochodzących z rozporządzenia Ministra Infrastruktury z dnia 14 września 2022 r. w sprawie minimalnych poziomów bezpieczeństwa brzegu morskiego oraz przebiegu granicznej linii ochrony brzegu morskiego,
- f. zmianę modelu danych dla obiektów infrastruktury portowej, dostępowej do portów oraz pozostałej, w celu dostosowania do możliwości prezentacji danych,
- g. zapewnienie użytkownikom możliwości importu danych własnych oraz eksportu warstw (w tym warstw użytkownika),
- h. udostępnienie narzędzia do prezentacji kartograficznej oraz umożliwienie dostępu do dużych zbiorów danych gromadzonych przez administrację morską, w tym możliwość publikacji profili batymetrycznych pozyskiwanych w ramach Monitoringu Brzegu Morskiego,
- i. opracowanie narzędzia do generowania profili terenów na podstawie danych z numerycznego modelu terenu (NMT) oraz utworzenie narzędzia do wizualizacji strat sztormowych na podstawie profili batymetrycznych,
- j. zapewnienie dostępu do danych zgromadzonych w SIPAM za pośrednictwem OGC API, w tym modernizacja modelu danych i interfejsów API opracowanych w ramach SIPAM,
- k. opracowanie aplikacji webowej, działającej również na urządzeniach mobilnych,
- l. zapewnienie monitoringu badań naukowych na polskich morskich wodach wewnętrznych, morzu terytorialnym i wyłącznej strefie ekonomicznej, realizowanych na podstawie pozwoleń wydanych w oparciu o ustawę z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej i zasilenie systemu danymi od 2017 r.,

- m. integrację z danymi pochodzącymi z komórek Elektronicznej Mapy Nawigacyjnej ENC,
- n. rozbudowa systemu o:
 - i. zamieszczenia informacji nt. obiektów technicznej ochrony brzegów;
 - ii. zamieszczenia wizualizacji analiz historycznej przebudowy brzegu i dna morskiego (analiza danych batymetrycznych i tachimetrycznych) dla lat, w których wykonywano pomiary (od 2004 r.);
 - iii. zamieszczenia informacji nt. projektów sztucznego zasilania wykonywanych na wybrzeżu (ilość i miejsce odkładu);
 - iv. zamieszczenia informacji nt. robót pogłębiarskich i podczyszczeniach wykonywanych w portach i torach podejściowych do portów (informacja przydatna z punktu widzenia oceny transportu osadu i tempa przebudowy brzegu) - tylko zaznaczenie tematu w części dot. ochrony brzegów morskich;
- 8) Opracowanie rejestru wymagań dla systemu SIPAM2 (wymagania funkcjonalne i нефункционалне);
- 9) Przedstawienie koncepcji wdrożenia systemu SIPAM2 (opis funkcjonalny z projektem architektury technicznej rozwiązania od strony sprzętowo systemowej, bazodanowej, aplikacyjnej);
- 10) Planowany czas trwania etapu analizy przedwdrożeniowej – 3 miesiące od dnia podpisania umowy.

2. Dostawa infrastruktury teleinformatycznej

2.1. Ogólne założenia dla środowiska systemu SIPAM2.

Rozwiązania sprzętowe i programowe umożliwiające budowę środowiska dla systemu SIPAM2 powinny obejmować:

- klaster wirtualizacyjny w DC1;
- redundantną sieć storage opartą na protokole iSCSI w DC1;
- redundantną sieć Ethernet LAN w DC1;
- lokalny system wykonywania i przechowywania kopii zapasowych w DC1;
- zdalną kopię zapasową przechowywaną w DC2;
- możliwość odtworzenia systemu SIPAM2 po awarii;
- centralne zarządzanie, monitoring i raportowanie.

Przedstawione wymagania mają charakter wstępny i nie przesądzają o wyborze konkretnego producenta, modelu urządzenia ani technologii, o ile proponowane rozwiązanie zapewni wymagany poziom funkcjonalności, dostępności, bezpieczeństwa i skalowalności.

Wszelkie nazwy własne, znaki towarowe, normy, aprobaty, specyfikacje techniczne, systemy lub technologie (w tym w szczególności oprogramowanie VMware, Proxmox VE, Veeam, Windows Server, PostgreSQL, Geoserver) użyte w niniejszym Opisie Przedmiotu Zamówienia zostały użyte wyłącznie w celu sprecyzowania wymogów funkcjonalnych, eksploatacyjnych lub technicznych oraz w celu określenia standardu wydajności i jakości oczekiwanej przez Zamawiającego.

Zamawiający dopuszcza w każdym przypadku zaoferowanie rozwiązań, sprzętu lub oprogramowania równoważnego pod względem wydajności, funkcjonalności, parametrów użytkowych, bezpieczeństwa oraz kompatybilności technologicznej ze środowiskiem Zamawiającego.

2.2. Środowisko wirtualizacyjne.

Środowisko dla systemu SIPAM2 planuje się oprzeć na technologii wirtualizacji. Wirtualizacja powinna umożliwić uruchamianie poszczególnych komponentów SIPAM2 w postaci odseparowanych maszyn wirtualnych oraz zapewnić elastyczne przydzielanie zasobów obliczeniowych, pamięciowych, dyskowych i sieciowych.

Wirtualizacja zapewni zwiększony poziom bezpieczeństwa, elastyczność zarządzania zasobami oraz możliwość łatwej rozbudowy infrastruktury w przyszłości. Zastosowanie maszyn wirtualnych pozwoli na logiczne odseparowanie poszczególnych komponentów systemu, niezależne przydzielanie zasobów obliczeniowych oraz uproszczenie procesów związanych z utrzymaniem, odtwarzaniem i migracją usług.

Środowisko wirtualne systemu SIPAM2 zostanie zbudowane z wykorzystaniem oprogramowania do wirtualizacji zainstalowanego na czterech nowych serwerach tworzących klaster aplikacyjny w DC1. Klaster aplikacyjny będzie przeznaczony do uruchamiania maszyn wirtualnych systemu SIPAM2 oraz innych usług wskazanych przez Zamawiającego.

Serwery backupowe będą stanowiły odrębne, fizyczne elementy infrastruktury i nie będą wchodziły w skład klastra aplikacyjnego.

Repozytoria kopii zapasowych w DC1 i DC2 będą wykorzystywały lokalne zasoby dyskowe serwerów backupowych. Wykonawca określi, czy repozytorium zostanie uruchomione na systemie fizycznym, czy w maszynie wirtualnej, oraz przedstawi sposób zapewnienia jego wydajności, odporności, bezpieczeństwa, możliwości rozbudowy i odtworzenia po awarii.

Planowane środowisko powinno umożliwiać:

- centralne zarządzanie hostami i maszynami wirtualnymi;
- tworzenie i modyfikowanie maszyn wirtualnych;

- obsługę wysokiej dostępności;
- automatyczne lub półautomatyczne odtwarzanie pracy maszyn po awarii hosta;
- migrację maszyn pomiędzy hostami, jeżeli będzie wymagana;
- obsługę współdzielonego storage'u blokowego iSCSI;
- obsługę wielościeżkowego dostępu do macierzy;
- integrację z systemem backupu;
- monitorowanie zasobów i zdarzeń;
- wykonywanie kopii konfiguracji platformy zarządzającej.

Obecnie środowisko wirtualizacyjne zbudowane jest w oparciu o VMware vSphere Standard 8. Dopuszcza się jednak zaoferowanie platformy opartej również na Proxmox VE lub innym rozwiązaniu klasy enterprise, pod warunkiem zapewnienia wymaganej dostępności, obsługi iSCSI, integracji z systemem backupu, wsparciem producenta oraz migracji z obecnie używanego rozwiązania.

2.3. Klaster serwerów.

Zamawiający zakłada budowę klastra złożonego z czterech nowych serwerów fizycznych, zlokalizowanych w DC1, przeznaczonych do uruchomienia nowego klastra aplikacyjnego oraz migracji maszyn wirtualnych ze starego klastra. Wskazana konfiguracja procesorów, liczby rdzeni i taktowania ma charakter orientacyjny i podlega optymalizacji przez Wykonawcę. Wykonawca może zaproponować inną konfigurację sprzętową, jeżeli zapewni ona wymaganą pojemność obliczeniową, pamięć operacyjną, możliwość obsługi awarii pojedynczego hosta, zgodność z oferowaną platformą wirtualizacyjną oraz korzystniejszy lub porównywalny całkowity koszt rozwiązania, uwzględniający licencje i wsparcie.

Planowana wyjściowa konfiguracja:

- dwa procesory po 24 rdzenie każdy;
- zegar bazowy procesorów nie niższy niż 2,9 GHz;
- łącznie minimum 48 rdzeni fizycznych;
- 512 GB pamięci RAM;
- możliwość dalszej rozbudowy pamięci RAM;
- dwa interfejsy 25 GbE przeznaczone do iSCSI;
- dwa interfejsy 25 GbE przeznaczone do sieci LAN;
- redundantne zasilacze;
- zdalny kontroler zarządzania;

- zgodność z proponowaną platformą wirtualizacyjną.

Nowy klaster powinien zapewniać co najmniej:

1. Uruchamianie maszyn wirtualnych wymaganych przez system SIPAM2 oraz inne wskazane przez Zamawiającego usługi.
2. Centralne zarządzanie hostami i maszynami wirtualnymi.
3. Wysoką dostępność maszyn wirtualnych.
4. Możliwość automatycznego lub półautomatycznego ponownego uruchomienia maszyn wirtualnych na innym hoście po awarii pojedynczego serwera.
5. Możliwość migracji maszyn wirtualnych pomiędzy hostami.
6. Dostęp do współdzielonej przestrzeni blokowej udostępnianej za pośrednictwem iSCSI.
7. Obsługę wielościeżkowego dostępu do przestrzeni iSCSI.
8. Możliwość wykonywania prac serwisowych bez konieczności wyłączania wszystkich maszyn wirtualnych.
9. Możliwość rozbudowy zasobów obliczeniowych i pamięciowych.
10. Integrację z systemem backupu.
11. Monitorowanie stanu serwerów, maszyn wirtualnych i zasobów klastra.
12. Eksport oraz odtwarzanie konfiguracji środowiska zarządzającego.

Jeżeli platforma wirtualizacyjna będzie umożliwiała funkcję automatycznego bilansowania obciążenia, dopuszcza się jej zastosowanie. Funkcja ta nie powinna jednak być traktowana jako bezwzględnie wymagana, jeżeli jej licencjonowanie powodowałoby nieuzasadniony wzrost kosztu rozwiązania.

Wymagania dotyczące zasobów.

Dobór serwerów powinien uwzględniać nie tylko bieżące wymagania systemu SIPAM2, ale również:

- zasoby aktualnie wykorzystywane przez maszyny wirtualne starego klastra;
- wzrost zapotrzebowania na CPU i RAM;
- rezerwę na awarię jednego hosta;
- zasoby potrzebne do migracji maszyn;
- okresowe zwiększenie obciążenia;
- uruchomienie dodatkowych usług infrastrukturalnych;
- wymagania systemu backupu i monitoringu, jeżeli komponenty te będą działały w klastrze.

Wykonawca powinien wykonać analizę pojemnościową na podstawie danych dostarczonych przez Zamawiającego. Analiza powinna zawierać co najmniej:

- aktualne zużycie CPU;
- aktualne zużycie pamięci RAM;
- maksymalne i średnie obciążenie;
- wymagania poszczególnych maszyn wirtualnych;
- wymaganą rezerwę;
- przewidywany wzrost obciążenia;
- liczbę maszyn możliwych do uruchomienia po awarii jednego hosta.

Przyjęte rozwiązanie powinno umożliwiać utrzymanie krytycznych maszyn wirtualnych po awarii pojedynczego serwera fizycznego.

Migracja

W ramach wdrożenia należy zaplanować migrację maszyn wirtualnych ze starego klastra do nowego klastra aplikacyjnego w DC1.

Zakres migracji powinien obejmować:

1. Inwentaryzację maszyn wirtualnych.
2. Inwentaryzację systemów operacyjnych, aplikacji i zależności.
3. Weryfikację wymagań CPU, RAM, storage i sieci.
4. Przygotowanie mapowania sieci VLAN.
5. Przygotowanie mapowania datastore'ów lub wolumenów.
6. Ustalenie kolejności migracji.
7. Identyfikację maszyn wymagających okna serwisowego.
8. Wykonanie kopii zapasowych przed migracją.
9. Przeprowadzenie migracji testowej.
10. Migrację maszyn produkcyjnych.
11. Weryfikację działania systemu SIPAM2 po migracji.
12. Przygotowanie procedury wycofania zmian.
13. Przekazanie raportu z migracji.

Jeżeli stara i nowa platforma będą kompatybilne, preferowana będzie migracja bez wyłączania maszyn wirtualnych.

Przed rozpoczęciem migracji Wykonawca powinien potwierdzić kompatybilność:

- wersji hypervisora;
- formatów maszyn wirtualnych;
- kontrolerów dysków wirtualnych;
- wersji narzędzi VMware Tools, Integration Services lub odpowiedników;
- kart sieciowych maszyn;
- systemów operacyjnych;
- mechanizmów backupu;
- konfiguracji VLAN i adresacji IP.

Odporność na uszkodzenia.

Wszystkie cztery serwery nowego klastra aplikacyjnego będą fizycznie zlokalizowane w DC1. Oznacza to, że klaster zapewni odporność na awarię pojedynczego serwera lub komponentu, ale nie zapewni odporności na całkowitą niedostępność DC1.

Odporność między lokalizacjami będzie realizowana przez:

- wykonywanie kopii zapasowych w DC1;
- przesyłanie drugiej kopii do DC2;
- możliwość odtworzenia maszyn wirtualnych z kopii przechowywanych w DC2;
- ewentualną replikację wybranych usług, jeżeli zostanie uznana za uzasadnioną.

Nie zakłada się budowy drugiego klastra wirtualizacyjnego w DC2 w ramach podstawowego wariantu rozwiązania.

2.4. Macierz produkcyjna iSCSI.

Dla klastra wirtualizacyjnego planuje się zastosowanie współdzielonej macierzy blokowej z dwoma kontrolerami i interfejsami iSCSI 25 GbE.

Macierz produkcyjna powinna zapewniać:

- dwa redundantne kontrolery;
- pracę po awarii pojedynczego kontrolera bez utraty dostępu do danych;
- redundantne interfejsy iSCSI 25 GbE;
- obsługę multipathingu;
- redundantne zasilacze i wentylatory;
- możliwość wymiany dysków bez wyłączania urządzenia;
- obsługę RAID5, RAID6 lub równoważnego mechanizmu ochrony danych;
- możliwość stosowania dysków hot spare;

- monitorowanie stanu dysków, kontrolerów, portów i zasilania;
- tworzenie wolumenów blokowych dla hostów wirtualizacyjnych;
- możliwość rozbudowy pojemności i liczby hostów;
- zgodność z proponowanym hypervisorem i systemem backupu.

Zamawiający zakłada dostawę macierzy produkcyjnej zapewniającej co najmniej 60 TB pojemności użytkowej dla środowiska wirtualizacyjnego, po uwzględnieniu zastosowanego poziomu ochrony danych, dysków hot spare oraz narzutów systemowych. Wykonawca może zaproponować inną organizację przestrzeni, w szczególności RAID6, RAID60, RAID10, pule dyskowe lub rozwiązanie równoważne, jeżeli zapewni ono wymaganą pojemność, dostępność, wydajność i możliwość rozbudowy. Pamięć masowa SSD oraz SAS 10K powinna być organizowana w odrębnych pulach lub warstwach, zgodnie z zaleceniami producenta macierzy i wymaganiami systemu SIPAM2. Podane wartości należy traktować jako wartości orientacyjne do konsultacji.

Dyski hot spare nie będą wliczane do wymaganej pojemności użytkowej. Wykonawca wskaże, czy zastosowano dyski hot spare dedykowane dla poszczególnych pul, czy globalne, oraz uzasadni przyjęte rozwiązanie.

Pojemność macierzy produkcyjnej nie obejmuje przestrzeni wymaganej do przechowywania kopii zapasowych. Repozytoria backupu zostaną zbudowane niezależnie, na lokalnych dyskach serwerów backupowych w DC1 i DC2.

2.5. Sieć iSCSI.

Dla zapewnienia wysokiej dostępności i wielościeżkowego dostępu do przestrzeni dyskowej planuje się zastosowanie dwóch niezależnych przełączników iSCSI o przepustowości 25/100 GbE.

Każdy przełącznik powinien posiadać:

- porty SFP28 25 GbE dla serwerów i macierzy;
- porty uplink 100 GbE lub równoważne;
- obsługę VLAN;
- obsługę jumbo frames;
- obsługę QoS;
- możliwość monitorowania portów i błędów transmisji;
- obsługę SNMPv3 lub równoważnego mechanizmu;
- możliwość rozbudowy;
- kompatybilność z interfejsami serwerów i macierzy.

Każdy host klastra powinien być podłączony do obu przełączników iSCSI, a macierz powinna udostępniać ścieżki przez oba przełączniki. Przełączniki powinny pracować jako dwa niezależne tory storage, a awaria jednego z nich nie może powodować utraty dostępu do danych.

Sieć iSCSI powinna być odseparowana od pozostałego ruchu za pomocą odrębnych VLAN-ów i podsieci. W konfiguracji hostów należy zastosować multipathing zgodny z wymaganiami producenta macierzy i hypervisor. Przy wielu interfejsach iSCSI należy stosować konfigurację zalecaną dla danego hypervisor, a nie traktować agregacji LACP jako zastępstwa dla multipathingu.

2.6. Sieć Ethernet LAN.

Niezależnie od dwóch przełączników iSCSI planuje się zastosowanie dwóch przełączników Ethernet LAN. Ich zadaniem będzie obsługa:

- sieci zarządzania;
- sieci maszyn wirtualnych;
- sieci migracji maszyn wirtualnych;
- ruchu backupowego;
- komunikacji z istniejącą siecią Zamawiającego;
- dostępu do usług infrastrukturalnych;
- komunikacji z systemami zewnętrznymi.

Proponowane wymagania dla przełączników Ethernet LAN:

- porty 25 GbE dla serwerów;
- porty uplink 40/100 GbE lub równoważne;
- obsługę VLAN 802.1Q;
- obsługę LACP;
- obsługę stackingu, MLAG, MC-LAG, virtual chassis lub rozwiązania równoważnego;
- routing warstwy 3, jeżeli będzie wymagany;
- obsługę QoS;
- obsługę ACL;
- obsługę RSTP/MSTP lub rozwiązania równoważnego;
- obsługę LLDP;
- monitorowanie przez SNMPv3, syslog i telemetrię;
- możliwość wykonania kopii konfiguracji;

- redundantne zasilanie, jeśli jest dostępne.

Każdy serwer klastra powinien mieć redundantne połączenie do obu przełączników LAN. Sieć maszyn wirtualnych, zarządzania, migracji i backupu powinna być logicznie rozdzielona za pomocą VLAN-ów i odrębnych podsieci.

Dopuszcza się wykorzystanie przełączników Ethernet LAN do obsługi ruchu backupowego. Nie zakłada się wykorzystywania przełączników iSCSI jako przełączników ogólnego przeznaczenia dla sieci użytkowników lub sieci maszyn wirtualnych.

2.7. System kopii zapasowej.

System backupu powinien zapewniać ochronę maszyn wirtualnych i pozostałych wskazanych obciążeń systemu SIPAM2. Wstępnie zakłada się ochronę co najmniej 50 obciążeń.

Planowana architektura obejmuje:

- główny serwer backupu w DC1;
- serwer pomocniczy lub repozytorium w DC2;
- repozytorium backupu w DC1;
- repozytorium backupu w DC2;
- lokalną przestrzeń dyskową w zatokach serwerów backupowych;
- kopię podstawową w DC1;
- kopię zdalną w DC2.

Oprogramowanie backupowe powinno umożliwiać:

- tworzenie kopii obrazowych maszyn wirtualnych;
- wykonywanie kopii pełnych i przyrostowych;
- stosowanie harmonogramów i retencji;
- kompresję i deduplikację;
- szyfrowanie kopii;
- wykonywanie backup copy do DC2;
- odtwarzanie całych maszyn;
- odtwarzanie pojedynczych plików;
- odtwarzanie dysków i wolumenów;
- odtwarzanie do innego hosta lub lokalizacji;
- wykonywanie kopii konfiguracji systemu backupu;

- generowanie raportów i powiadomień;
- kontrolę dostępu opartą na rolach;
- ochronę kopii przed przypadkowym lub nieuprawnionym usunięciem;
- integrację z repozytorium immutable, jeżeli zostanie przewidziane w oferowanym wariancie.

Proponowane jest rozwiązanie do kopii zapasowej Veeam lub innego oprogramowania klasy Veeam Backup & Replication, które umożliwia ochronę maszyn wirtualnych, fizycznych i chmurowych oraz obsługuje role backup server, proxy i repository.

Repozytoria backupu w serwerach.

W każdym centrum przetwarzania danych należy przewidzieć jeden dedykowany serwer backupowy.

Planowana konfiguracja serwerów, co najmniej:

- jeden procesor 16-rdzeniowy o taktowaniu bazowym nie niższym niż 2,0 GHz;
- 64 GB RAM;
- możliwość rozbudowy pamięci;
- dwa interfejsy 25 GbE;
- dwa dyski SSD 1,92 TB w RAID1 na system operacyjny i komponenty backupu;
- zatoki dyskowe na lokalne repozytorium;
- kontroler RAID obsługujący wymaganą liczbę dysków;
- redundantne zasilacze;
- zdalne zarządzanie sprzętowe;
- możliwość wymiany dysków i zasilaczy podczas pracy;
- kompatybilność z systemem backupu.

W DC1 przewiduje się uruchomienie głównego serwera zarządzającego oprogramowaniem backupowym oraz lokalnego repozytorium. W DC2 planuje się uruchomienie repozytorium zdalnego oraz komponentów potrzebnych do obsługi kopii zdalnych i odtwarzania.

Dopuszcza się zastosowanie repozytorium niezmiennego, repozytorium odseparowanego logicznie i administracyjnie, pamięci obiektowej z funkcją Object Lock, nośników offline albo rozwiązania równoważnego.

Przestrzeń repozytoriów backupu w DC1 i DC2 powinna zostać zbudowana z wykorzystaniem dysków lokalnych zainstalowanych w zatokach dyskowych w serwerach backupowych.

Każdy serwer backupowy powinien posiadać:

- dodatkowe zatoki na dyski przeznaczone do przechowywania kopii;
- możliwość zastosowania dysków SAS lub SATA klasy enterprise;
- sprzętowy kontroler RAID albo rozwiązanie równoważne;
- możliwość zastosowania RAID6 lub innego mechanizmu zapewniającego odporność na awarię co najmniej dwóch dysków;
- minimum dwa dyski hot spare albo możliwość ich zastosowania;
- możliwość wymiany dysków bez wyłączania serwera;
- monitorowanie stanu dysków i macierzy;
- możliwość rozbudowy pojemności;
- wydajne połączenie sieciowe 25 GbE;
- oddzielenie dysków systemowych od dysków repozytorium.

Przyjmuje się, że podstawą do wymiarowania repozytorium backupu jest maksymalnie 60 TB danych objętych ochroną.

Zakłada się nie mniej niż 120 TB użytkowej przestrzeni repozytorium backupu w każdej lokalizacji dla retencji 14 dni oraz nie mniej niż 150 TB użytkowej przestrzeni repozytorium backupu w każdej lokalizacji dla retencji 30 dni. Wymagana pojemność oznacza przestrzeń dostępną po zastosowaniu RAID lub technologii równoważnej, po uwzględnieniu dysków hot spare i narzutów systemowych.

Dyski repozytorium powinny być fizycznie odseparowane od dysków systemowych. Nie zaleca się przechowywania kopii backupowych na tych samych wolumenach, na których znajdują się system operacyjny, baza danych i pliki aplikacyjne oprogramowania backupowego.

2.8. Licencje.

Zakłada się wykorzystanie Microsoft Windows Server 2022 Standard na serwerach backupowych. Wykonawcy mogą zaproponować inne rozwiązanie, jeżeli oprogramowanie backupowe zapewnia pełną funkcjonalność na alternatywnym systemie operacyjnym i rozwiązanie będzie korzystniejsze kosztowo lub technicznie.

W przypadku pozostałych serwerów wykorzystywane będą systemy oparte na oprogramowaniu open source.

2.9. Wdrożenie.

Planowany czas realizacji zamówienia wynosi do sześciu miesięcy od dnia podpisania umowy, zgodnie z ustalonym z Wykonawcą harmonogramem dostaw, instalacji, konfiguracji, testów i odbioru.

Planowane zestawienie przedstawia poniższa tabela:

Lp.	Element	Założenia	Ilość
1	Serwer klastra wirtualizacyjnego	2 CPU po 24 rdzenie, 512 GB RAM, 2 × 25 GbE iSCSI, 2 × 25 GbE LAN	4
2	Macierz produkcyjna	2 kontrolery, iSCSI 25 GbE, SSD RI i SAS 10k, RAID5/RAID6, hot spare,	1
3	Przełącznik iSCSI	25/100 GbE, porty SFP28, redundancja, VLAN, jumbo frames, QoS	2
4	Przełącznik Ethernet LAN	25/100 GbE, VLAN, LACP, stacking/MLAG, routing, ACL, QoS	2
5	Serwer backupowy	1 CPU 16 rdzeni, 64 GB RAM, 2 × 25 GbE, 2 × SSD 1,92 TB RAID1, lokalne zatoki backupowe	2
6	Dyski repozytorium backupu	Dyski SAS/SATA enterprise w zatokach serwerów backupowych, RAID6/RAIDZ2 lub rozwiązanie równoważne	2
7	Oprogramowanie backupowe	Ochrona 50 obciążeń, kopia lokalna i zdalna, restore, raportowanie	50
8	Okablowanie i optyka	SFP28, QSFP28, SR, DAC/AOC, patchcordy, oznaczenia	1
9	Licencje wirtualizacyjne	Hypervisor, zarządzanie centralne, HA i migracja	-
10	Wdrożenie	Projekt, montaż, konfiguracja, testy, dokumentacja i szkolenie	-

3. Gwarancja i usługi wsparcia technicznego dla infrastruktury teleinformatycznej:

- 1) Gwarancja i wsparcie techniczne w okresie pięciu lat od daty odbioru infrastruktury teleinformatycznej;
- 2) Wsparcie techniczne będzie realizowane przez producenta lub autoryzowanego partnera producenta;
- 3) Czas reakcji w ramach wsparcia nie gorszy niż Next Business Day (NBD);
- 4) Możliwość zgłaszania incydentów 24 godziny na dobę, 7 dni w tygodniu (minimum dla incydentów krytycznych);
- 5) Dostęp do aktualizacji firmware'u i oprogramowania systemowego w okresie trwania gwarancji.

4. Dostawa i wdrożenie systemu informatycznego SIPAM2

Zamawiający w ramach zamówienia planuje zmodernizować oraz rozbudować funkcjonalność systemu SIPAM oraz wdrożyć jego wersję produkcyjną jako system SIPAM2, z uwzględnieniem następujących aspektów:

- 1) System SIPAM2 będzie realizował wymagania określone w analizie przedwdrożeniowej;
- 2) Wdrożenie systemu SIPAM2 zostanie wykonane na infrastrukturze teleinformatycznej dostarczonej zgodnie z pkt 2;
- 3) Wszystkie dane Zamawiającego muszą być przetwarzane wyłącznie w obrębie infrastruktury (w tym, bazy danych) Zamawiającego, bez możliwości transferu danych poza infrastrukturę Zamawiającego;
- 4) Edycja danych w SIPAM2 będzie możliwa tylko dla uwierzytelnionych użytkowników;
- 5) System musi rejestrować operacje utworzenia, modyfikacji, usunięcia, importu i eksportu danych oraz zmiany uprawnień. Rejestr musi zawierać co najmniej identyfikator użytkownika lub systemu, datę i czas, rodzaj operacji, obiekt, zakres zmiany oraz wartości przed i po zmianie, o ile jest to technicznie możliwe. Rejestr audytowy musi być chroniony przed modyfikacją przez zwykłych użytkowników i administratorów aplikacji.
- 6) SIPAM2 w środowisku produkcyjnym będzie skonfigurowany do tworzenia automatycznych cyklicznych kopii bezpieczeństwa, które będą umożliwiać jego odtworzenie w wypadku awarii;
- 7) Środowisko testowe SIPAM2 będzie odzwierciedlało środowisko produkcyjne i służyło do bezpiecznego testowania oprogramowania po wprowadzeniu aktualizacji i poprawek a przed ich wdrożeniem na środowisku produkcyjnym. Administrator systemu będzie miał możliwość replikowania środowiska testowego na podstawie środowiska produkcyjnego w dowolnym momencie;

- 8) Wykonawca przeprowadzi testy bezpieczeństwa aplikacji, obejmujące co najmniej testy uwierzytelniania, autoryzacji, zarządzania sesją, walidacji danych, ochrony API, kontroli dostępu do danych przestrzennych oraz odporności na podatności aplikacyjne. Raport zawierający wyniki testów i plan usunięcia stwierdzonych podatności zostanie przekazany Zamawiającemu.
- 9) Wykonawca opracuje i prześle Zamawiającemu dokumentację użytkownika (instrukcja obsługi systemu), dokumentację administratora (instalacja, konfiguracja, monitoring, archiwizacja, bezpieczeństwo), dokumentację bazy danych (opis modelu danych, model fizyczny modelu danych);
- 10) Wykonawca przeprowadzi szkolenia dla użytkowników SIPAM2 obejmujące kluczowe funkcjonalności systemu;
- 11) Wykonawca przeprowadzi szkolenia dla administratorów technicznych w zakresie licencjonowania, architektury i konfiguracja systemu/aplikacji, zarządzania bazą danych, zarządzania na poziomie aplikacji, reguły zabezpieczeń, czynności administracyjne, nadawanie uprawnień użytkownikom;
- 12) Zamawiający dopuszcza przeprowadzenie szkoleń w siedzibie Zamawiającego oraz w formie zdalnej;
- 13) Wykonawca udzieli Zamawiającemu licencji/certyfikatu na nieograniczone terminowo użytkowanie systemu SIPAM2;
- 14) Wykonawca udzieli Zamawiającemu licencji/certyfikatu na użytkowanie oprogramowania osób trzecich, które będzie konieczne do uruchomienia i funkcjonowania systemu SIPAM2;
- 15) Prawa autorskie do dokumentacji, opracowań, prezentacji powstałych w trakcie dostawy i wdrożenia zostaną przeniesione na Zamawiającego;
- 16) Planowany czas wdrożenia systemu SIPAM2 – 12 miesięcy od dnia podpisania umowy.

5. Migracja danych do SIPAM2

Migracja danych z SIPAM do nowego rozwiązania uwzględnieni następujące aspekty:

- 1) Migracji podlegają dane zawarte w bazach danych, dokumenty, dane rastrowe oraz pozostałe pliki stanowiące repozytorium systemu SIPAM;
- 2) Migracja danych musi odbyć się bez utraty integralności i kompletności danych;
- 3) Migracja danych musi być zaplanowana i wykonana w sposób minimalizujący wpływ na bieżącą działalność Zamawiającego;
- 4) Migracja danych musi zostać poprzedzona opracowaniem szczegółowego harmonogramu uzgodnionego z Zamawiającym;

- 5) Wykonawca ponosi pełną odpowiedzialność za ewentualne błędy, utratę danych lub nieprawidłowe działanie systemów wynikające z procesu migracji;
- 6) Stwierdzone przez Wykonawcę błędy w danych źródłowych nie podlegają naprawie przez Wykonawcę;
- 7) Wykonawca zobowiązany jest do zabezpieczenia pozyskanych od Zamawiającego migrowanych danych w sposób, który uniemożliwi osobom nieupoważnione ich pozyskanie;
- 8) Wykonawca nie jest upoważniony do przekazywania danych z migracji innym podmiotom;
- 9) Przed przystąpieniem do procesu migracji Wykonawca utworzy ich kopię zapasową;
- 10) Po zakończeniu migracji Wykonawca prześle oświadczenie lub protokół potwierdzający usunięcie danych Zamawiającego i ich kopii z systemów, urządzeń, repozytoriów tymczasowych oraz środowisk podwykonawców, z wyjątkiem danych, których zachowanie wynika z bezwzględnie obowiązujących przepisów prawa.
- 11) Wykonawca opracuje i przeprowadzi testy migracji danych:
 - a. jakościowe (zachowana poprawność, integralność, kompletność danych)
 - b. ilościowe (zachowana liczba rekordów oraz sumy kontrolne przed i po migracji)
- 12) Raport z testów migracji zostanie przekazany Zamawiającemu;
- 13) Prognozowany czas migracji danych do SIPAM2 – 12 miesięcy od dnia podpisania umowy.

6. Usługi serwisu gwarancyjnego SIPAM2 oraz wsparcia technicznego SIPAM2

W ramach planowanego zamówienia Wykonawca będzie świadczył usługi serwisu gwarancyjnego z uwzględnieniem następujących aspektów:

- 1) Usługi serwisu gwarancyjnego będą polegały na realizacji przez Wykonawcę zgłoszeń gwarancyjnych dotyczących funkcjonowania systemu SIPAM2;
- 2) Każde zgłoszenie będzie klasyfikowane według następujących kryteriów:
 - a. błąd krytyczny – zdarzenie, które uniemożliwia Zamawiającemu świadczenie którejkolwiek z usług SIPAM2;
 - b. błąd ważny – zdarzenie, które negatywnie wpływa na wydajność i funkcjonalność SIPAM2, lecz nie uniemożliwia Zamawiającemu świadczenia jakichkolwiek usług SIPAM2. Wszelkie zdarzenia negatywne, których wystąpienie uzależnione będzie od danych

zgrupowanych w bazach danych SIPAM2, będą klasyfikowane jako błąd ważny;

- c. poprawka – występowanie błędów, niekompletności lub nieaktualności w tym w dokumentacji SIPAM2;
- 3) Czas realizacji poszczególnych rodzajów zgłoszeń będzie wynosił:
- a. błąd krytyczny – 24 godziny zegarowe,
 - b. błąd ważny – 5 dni roboczych,
 - c. poprawka – 10 dni roboczych;
- 4) Wykonawca będzie utrzymywał oraz udostępniał Zamawiającemu system obsługi zgłoszeń gwarancyjnych, który będzie umożliwiał podstawową komunikację (w tym przysyłanie załączników) pomiędzy Zamawiającym i Wykonawcą dotyczącą usług serwisu gwarancyjnego.
- 5) Usługi serwisu gwarancyjnego będą świadczone przez Wykonawcę w dni robocze w godzinach od 7:30 do 15:30;
- 6) Okres świadczenia usługi serwisu gwarancyjnego rozpocznie się od dnia odbioru SIPAM2 i będzie trwał przez 24 kolejne miesiące.

W ramach planowanego zamówienia Wykonawca będzie świadczył usługi serwisu wsparcia technicznego z uwzględnieniem następujących aspektów:

- 1) Usługi serwisu wsparcia technicznego będą polegały na realizacji przez Wykonawcę zgłoszeń serwisowych dotyczących funkcjonowania systemu SIPAM2;
- 2) Usługi serwisu wsparcia technicznego będą wyceniane i rozliczane w tzw. punktach wsparcia. Cena jednego punktu wsparcia będzie zaoferowana przez Wykonawcę w trakcie postępowania o udzielenie zamówienia publicznego;
- 3) Każde zgłoszenie serwisowe będzie wyceniane przez Wykonawcę w punktach wsparcia. Po zaakceptowaniu przez Zamawiającego wyceny, Wykonawca będzie przystępował do realizacji zgłoszenia;
- 4) Każde zgłoszenie będzie klasyfikowane według następujących kryteriów:
 - a. błąd krytyczny – zdarzenie, które uniemożliwia Zamawiającemu świadczenie którejkolwiek z usług SIPAM2;
 - b. błąd ważny – zdarzenie, które negatywnie wpływa na wydajność i funkcjonalność SIPAM2, lecz nie uniemożliwia Zamawiającemu świadczenia jakichkolwiek usług SIPAM2. Wszelkie zdarzenia negatywne, których wystąpienie uzależnione będzie od danych zgromadzonych w bazach danych SIPAM2, będą klasyfikowane jako błąd ważny;

- c. poprawka – występowanie błędów, niekompletności lub nieaktualności w tym w dokumentacji SIPAM2 oraz ulepszanie funkcjonalności systemu, w tym dodawanie nowych funkcji i rozbudowa jego zasobu danych oraz aktualizacja oprogramowania systemowego, w tym w zakresie poprawek bezpieczeństwa;
- 5) Czas realizacji poszczególnych rodzajów zgłoszeń będzie wynosił:
- a. błąd krytyczny – 24 godziny zegarowe,
 - b. błąd ważny – 5 dni roboczych,
 - c. poprawka – minimum 10 dni roboczych;
- 6) Wykonawca będzie utrzymywał oraz udostępniał Zamawiającemu system obsługi zgłoszeń serwisowych, który będzie umożliwiał podstawową komunikację (w tym przysyłanie załączników) pomiędzy Zamawiającym i Wykonawcą dotyczącą usług serwisu gwarancyjnego.
- 7) Usługi serwisu wsparcia technicznego będą świadczone przez Wykonawcę w dni robocze w godzinach od 7:30 do 15:30;
- 8) Okres świadczenia usługi wsparcia technicznego rozpocznie się od dnia odbioru SIPAM2 i będzie trwał do wyczerpania punktów wsparcia;
- 9) Po zakończeniu każdego okresu rozliczeniowego, trwającego do końca danego kwartału, Wykonawca będzie przekazywał Zamawiającemu rejestr punktów wsparcia, zawierający wykaz wszystkich zgłoszeń serwisowych wraz z:
- a. oznaczeniem okresu rozliczeniowego,
 - b. tematami zgłoszeń serwisowych,
 - c. datami rozpoczęcia i datami zakończenia danego zgłoszenia,
 - d. ilością punktów wsparcia, które zostały wykorzystane do realizacji danego zgłoszenia,
 - e. sumaryczną ilością punktów wsparcia wykorzystaną w danym okresie rozliczeniowym,
 - f. ilością punktów wsparcia, które pozostały do wykorzystania;
- 10) Po zakończeniu każdego okresu rozliczeniowego, na podstawie rejestru punktów wsparcia Zamawiający będzie przygotowywał protokół odbioru prac.

III. Pozostałe planowane postanowienia w stosunku do przedmiotu zamówienia i sposobu jego wykonania

- 1) Wszystkie prace w ramach realizacji przedmiotu zamówienia będą wykonywane we współpracy z Zamawiającym;

- 2) Wykonawca jest zobowiązany w trakcie realizacji wszystkich prac do przestrzegania polityk oraz regulaminów bezpieczeństwa informacji obowiązujących w Ministerstwie Infrastruktury, Urzędzie Morskim w Gdyni, Urzędzie Morskim w Słupsku i Urzędzie Morskim w Szczecinie;
- 3) Wykonawca zobowiązany jest przestrzegać wytycznych dotyczących ochrony danych osobowych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz zawrzeć z Zamawiającym umowę na przetwarzanie danych osobowych określających warunki ich przetwarzania;
- 4) Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych przez Wykonawcę w ramach realizacji przedmiotu zamówienia (m.in. w czasie dostawy infrastruktury, instalacji oprogramowania, konfiguracji i wdrożenia);
- 5) Zamawiający dopuszcza realizację prac, niewymagających osobistego uczestnictwa personelu Wykonawcy, zdalnie, na zasadach obowiązujących u Zamawiającego w kontekście polityki bezpieczeństwa oraz zasad przetwarzania danych, po wcześniejszym uzgodnieniu z Zamawiającym;
- 6) Warunkiem przystąpienia do realizacji zamówienia jest podpisanie przez Wykonawcę oświadczenia o zachowaniu w tajemnicy danych osobowych;
- 7) Komunikacja z Zamawiającym musi odbywać się w języku polskim;
- 8) Cała dostarczona dokumentacja musi być sporządzona w języku polskim, chyba że Zamawiający udzieli zgody na wydanie części dokumentacji technicznej w języku angielskim;
- 9) Zamawiający po zawarciu umowy udostępni Wykonawcy wszelką dokumentację związaną z systemem SIPAM oraz umożliwi dostęp do systemu do celów, które będą służyć jedynie realizacji przedmiotu umowy;
- 10) Pozytywny protokół odbioru każdego z etapów będzie podstawą do wystawienia przez Wykonawcę faktury za realizację prac w danym etapie.