Załącznik nr 1 – Opis przedmiotu zamówienia.

Przedmiot Zamówienia
Przedmiotem Zamówienia jest udostępnienie dedykowanego serwera wraz usługami utrzymania infrastruktury przez okres 30 miesięcy.

Całość rozwiązania ma być dostarczona w modelu usługowym.
Oferent, będzie świadczył usługę dla Zamawiającego siedem dni w tygodniu i 24 godziny na dobę (łącznie przez okres 30 miesięcy).

I. Wymagania technologiczne:

Projekt obejmuje udostępnienie infrastruktury dedykowanej, w postaci serwera dedykowanego (dalej określonego jako infrastruktura dedykowana), spełniającej następujące wymagania:

Procesor: dwa minimum dwunasto-rdzeniowe procesory przeznaczony do zastosowań serwerowych o architekturze CISC, obsługujące (pojedynczo) do 768GB pamięci operacyjnej DDR4 z korekcją błędów, parowanej w czterech kanałach, zużywające nie więcej niż 200W per procesor.

Pamięć operacyjna: Minimum 256GB pamięci operacyjnej DDR4 z korekcją błędów.

Przestrzeń dyskowa: Sprzętowa macierz dyskowa z potrzymaniem bateryjnym oraz 2GB pamięci podręcznej, obsługująca macierze poziomów: 0, 1, 5, 6, 50, 60. Minimum 1200GB przestrzeni dyskowej, skonfigurowanej w RAID10 na dyskach o prędkości minimum 10000obr/s. Serwer powinien posiadać minimum 12 slotów na dyski twarde wielkości 3,5".

Karta sieciowa: Serwer wyposażony w cztery porty Gigabit-Ethernet

Zasilanie: Minimum dwa redundantne zasilacze, umożliwiające ich wymianę bez wyłączania serwera (Hot-Swap) o minimalnej mocy 980W każdy.

Zarządzanie zdalne: Możliwość zdalnego zarządzania serwerem z panelu WWW oraz powłoki, za pośrednictwem sieci.

Rodzaj obudowy: RACK

Szyny montażowe: Ruchome

System operacyjny: Zamawiający zamierza użyć własnych licencji Windows systemu operacyjnego.

Wymagania dla komponentów infrastruktury:

Wymagania co do serwera:

- Redundantne podłączenie do sieci LAN (wykorzystywane co najmniej 4 interfejsy o przepustowości co najmniej 10Gbit/s każdy).
- Redundantne podłączenie do sieci SAN (wykorzystywane co najmniej 2 interfejsy o przepustowości co najmniej 8Gbit/s każdy).
- Redundantne zasilacze podłączone do dwóch niezależnych torów zasilania.
- Co najmniej dwa procesory , każdy co najmniej 12 rdzeniowy o nominalnej częstotliwości taktowania nie mniejszej niż 2,5GHz uzyskujący w teście PassMark wynik:
    - PassMark - CPU Mark nie mniejszy niż 1867 dla jednego procesora
- Pamięć RAM typu DDR4 o częstotliwości pracy co najmniej 2133 Mhz.
- Dedykowany, dodatkowy port fizyczny do zarządzania serwerem.

Minimalne wymagania dla warstwy sieciowej:

- Połączenie do sieci Internet o przepustowości minimum 5Mbit/s
- Dostępna adresacja IPv4 (Minimum jeden zewnętrzny adres IPv4).
- Możliwość zarządzania serwerem za pośrednictwem portu zarządzania po zestawieniu VPN.

Wymagania dla macierzy dyskowych:

Macierze dyskowe:

- Brak pojedynczego punktu awarii, który powodowałby brak dostępu do danych.
- Redundantne zasilacze podłączone do dwóch niezależnych torów zasilania
- Udostępnienie wolumenów o wielkości co najmniej 1,2 TB.
- Każdy serwer fizyczny musi mieć dostęp do zasobów dyskowych po sieci o przepustowości minimalnej 8 Gbit/s co najmniej dwoma niezależnymi drogami (brak pojedynczych punktów awarii).
- Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID0+1, RAID1, RAID5 i RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich typów dysków twardych, w tym SSD.
- Co najmniej cztery kontrolery pracujące w trybie active/active. Równoczesny, aktywny dostęp (odczyt/zapis) do każdego dysku logicznego (LUN) ze wszystkich kontrolerów macierzy dla lepszego rozłożenia obciążenia
- Możliwość dynamicznego zwiększania pojemności woluminów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych.
- Macierz musi umożliwiać migrację danych, bez przerywania do nich dostępu, pomiędzy różnymi warstwami technologii dyskowych: EFD/SSD, FC/SAS, MDL SAS/SATA oraz różnych poziomów RAID na poziomie całych woluminów logicznych, jak również na poziomie części woluminów logicznych.
- Macierz musi zapewniać wydajność na poziomie co najmniej 20 000 IOPS dla ruchu losowego przy rozkładzie R/W (60%/40%).
- Przestrzeń dyskowa udostępniana przez macierz musi być replikowana do innej macierzy nie rzadziej niż co 8 godzin.

Wymagania dla zarządzania oraz monitoringu:

Wymagania dla udostępnianych Zamawiającemu mechanizmom monitoringu systemu:

Wykonawca zapewni Zamawiającemu dostęp do graficznego system monitoringu prezentującego co najmniej statystyki (poprzez jeden interfejs) dotyczące:

- wykorzystanie interfejsów sieciowych,
- dostępności łącz,
- błędy na interfejsach sieciowych,
- liczba uruchomionych procesów,
- logów systemowych,
- aplikacji poprzez język skryptowy.

System musi zapewniać monitoring powyższych parametrów dla udostępnionego środowiska w trybie ciągłym.

W celu określenia trendów dotyczących wykorzystania zasobów, okres przechowywania statystyk nie może być krótszy niż okres 2 lat dla maszyny.

Wymagania dotyczące możliwości przechowywania danych:

- Dane maszyn muszą być przechowywane na macierzach dyskowych zgodnych z wymaganiami opisanymi powyżej w sposób zapewniający ich dostępność w przypadku awarii jednego komponentu macierzy takiego jak, dysk, kontroler macierzowy, zasilacz.
- Przechowywane dane muszą być zabezpieczone w sposób zgodny co najmniej z RAID 5. Dopuszcza się zastosowanie RAID 10.
- W celu podniesienia bezpieczeństwa danych, muszą one być replikowane do drugiej macierzy nie rzadziej niż co 8 godzin. Poziom zabezpieczenia danych nie może być niższy niż RAID5.
- Dane systemów produkcyjnych muszą być zabezpieczone przez systemem tworzenia kopii bezpieczeństwa.
- Kopie zapasowe muszą być wykonywane w modelu D2D2T.
- Kopia pełna wykonywana co najmniej dwa razy w tygodniu.
- Zamawiający wymaga by pełna kopia danych była przechowywana w obu ośrodkach przetwarzania danych – w ośrodku podstawowym oraz zapasowym, który jest oddalony od podstawowego centrum o co najmniej 20 kilometrów, nie dalej jednak niż 50 km. Dane systemu tworzenia kopii bezpieczeństwa muszą być przechowywane na innych urządzeniach niż dane produkcyjne.
- Oprogramowanie systemu tworzenia kopii zapasowych musi zapewnić możliwość wykonywania kopii bezpieczeństwa dla całego środowiska udostępnionego Zamawiającemu.
- Oprogramowanie musi umożliwiać wykonywanie backupów dla systemów: Linux oraz Windows.
- Do przechowywania danych wykorzystywane muszą być dyski oraz bezobsługowe biblioteki taśmowe.

- Każda biblioteka taśmowa używana do przechowywania kopii zapasowych musi posiadać pojemność 500 TB bez kompresji (native) i musi pozwalać na rozbudowę do 2 PB.
- System musi zapewnić możliwość odtworzenia danych w przypadku ich utraty.
- System musi zapewnić możliwość tworzenia kopii zapasowych zarówno na dyski jak i na napędy taśmowe.
- System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
- System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. Multistreaming.
- System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows.
- System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL.
- System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania.
- Zaproponowane rozwiązanie musi pozwalać na nielimitowany backup dowolnej ilości serwerów Windows/Linux wraz z nielimitowaną ilością aplikacji na tych serwerach zainstalowanych, wraz z mechanizmem deduplikacji danych i replikacji do innych lokalizacji.
- Dane kopii zapasowych nie pomniejsza storage określonego w wymaganiach dla projektu. Miejsce na dane backupowe zapewnia Wykonawca z zapewnieniem bezpieczeństwa przechowywanych kopii oraz gwarancją odtworzenia.

Wymagania dotyczące utrzymania sytemu i poziomu dostępności usług:

Wykonawca zapewnia pełną gwarancję na dostarczone produkty oraz wykonane usługi w ramach dostarczenia platformy, w całym okresie trwania umowy.

- Dane - wszelkie informacje, w jakiejkolwiek postaci przekazane do Wykonawcy w związku z Umową.
- SLA (Service Level Agreement) - Gwarancja Jakości Usług Informatycznych.
- Awaria - czasowy brak dostępności Usług Informatycznych. Przez brak dostępu do Usług rozumiany jest całkowity brak możliwości korzystania z Usług przez Zamawiającego.
- Problem - czasowy brak dostępności Usług Informatycznych. Przez brak dostępu do Usług rozumiany jest częściowy brak możliwości korzystania z Usług przez część użytkowników lub brak możliwości korzystania z części funkcjonalności.
- Przerwa Techniczna – czasowy brak dostępu do usług związany z koniecznością przeprowadzenia niezbędnych prac konserwacyjnych, zaplanowany i zapowiedziany przez Wykonawcy.
- Zespół Operatorów - wyszkolony personel Wykonawcy monitorujący przez 24 h na dobę dostępność Usług Informatycznych.
- Czas Reakcji - oznacza maksymalny okres czasu, który może upłynąć od momentu Zgłoszenia Awarii lub Problemu przez Zamawiającego do czasu udzielenia odpowiedzi przez dyżurujący Zespół Operatorów

- Czas Naprawy - oznacza maksymalny okres czasu, który może upłynąć od momentu Wystąpienia Awarii lub Problemu do czasu przywrócenia jakości świadczonych Usług do stanu sprzed Awarii lub Problemu.
- Parametry SLA
    - Czasu Reakcji 15 minut.
    - Usunięcie przyczyn Awarii w przeciągu 2 godzin dla Awarii i 6 godzin dla Problemu. Wykonawca musi zagwarantować działanie Usług w skali roku na poziomie 99,95% dla Usług. Parametr liczony w okresie 12 miesięcy od daty uruchomienia Usługi. Parametr wyrażony w procentach.
- Przerwy Techniczne
    - Wykonawca musi poinformować Zamawiającego o terminach planowanych Przerw Technicznych w świadczeniu Usług Informatycznych z co najmniej 72 godzinnym wyprzedzeniem.
- Stosowanie SLA jest wyłączone w przypadku:
- a) wystąpienia Przerwy Technicznej,
- b) wystąpienia Awarii lub Problemu której przyczyną jest samodzielne działanie Zamawiającego lub osoby trzeciej (podwykonawcy działającego na zlecenie Zamawiającego), za które Wykonawca nie ponosi odpowiedzialności,
- c) wystąpienia Awarii lub Problemu wynikającej z nieprawidłowego funkcjonowania:
    - sieci komputerowej Zamawiającego w szczególności połączenia z siecią Internet,
    - błędnej konfiguracji urządzeń za pomocą których użytkownicy Zamawiającego korzystają z Usług,
    - błędnej konfiguracji urządzeń sieci komputerowej Zamawiającego,
    - zablokowania dostępu użytkowników do ogólnoświatowej sieci Internet będący konsekwencją działań tego użytkownika w sieci Internet.
- Wykonawca w ramach usługi zapewni dostęp do usługi HelpDesk:
    - w trybie 24/7 zapewni telefoniczne wsparcie umożliwiające zgłaszanie usterek i awarii systemów,
    - Po zgłoszeniu Wykonawca doda zgłoszenie do systemu zgłoszeniowego,
    - Zapewni telefoniczne konsultacje merytoryczne przy rozwiązywaniu problemów w trybie 24/7.
- Całość komunikacji Zamawiającego z HelpDesk (system obsługi zgłoszeń) oraz komunikacja z inżynierami i osobami obsługującymi Call Center Wykonawcy musi odbywać się w języku polskim.

II. <u>Wymagania dla komponentów infrastruktury według parametrów:</u>

1. Lokalizacja

- Teren na którym zlokalizowane jest CPD (wszystkie budynki i instalacje) musi być ogrodzony z zapewnieniem bezpiecznej strefy buforowej.
- CPD musi być zaprojektowane i zbudowane z właściwym przeznaczeniem (serwerownia, centrum przetwarzania danych, ośrodek przetwarzania danych, data center).
- Szerokość strefy buforowej (od ścian budynku do ogrodzenia) nie mniejsza niż 10m.

- W strefie buforowej nie mogą znajdować się drzewa oraz inna roślinność pozwalająca na rozprzestrzenianie się ognia.
- Wysokość ogrodzenia Terenu nie większa niż 170cm.
- Na ogrodzonym Terenie, na którym zlokalizowane jest CPD, mogą znajdować się tylko budynki i instalacje bezpośrednio związane z działalnością CPD.
- CPD nie może pełnić innych funkcji użytkowych, poza funkcjami bezpośrednio związanymi z elektronicznym przetwarzaniem danych.
- Obiekt CPD musi znajdować się w całości powyżej poziomu gruntu, na którym został wzniesiony.
- Obiekt CPD musi być fizycznie niezależnym budynkiem lub budynkami.
- Odległość od stacji paliw oraz składów paliw płynnych (w linii prostej) większa niż 0,5km.
- Odległość od najbliższych obiektów/miejsc skupisk ludzkich (powyżej 1000 osób: stadiony, centra handlowe, fabryki) większa niż 5km.
-
- CPD musi być położone na Terenie niezagrożonym powodzią lub podtopieniem. Położenie całego Terenu poza obszarem zagrożonym podtopieniem musi zostać wykazane badaniami obejmującymi modelowanie hydrologiczne zagrożenia podtopieniami ze strony najbliższego cieku wodnego.
- Odległość od obiektów stanowiących potencjalny cel ataków terrorystycznych (budynki administracji centralnej i rządowej, bazy wojskowe, szpitale, centra rozrywki, lotniska, uczelnie wyższe, dworce kolejowe) większa niż 1km.
- Odległość w linii prostej pomiędzy ośrodkiem podstawowym i zapasowym nie miej niż 20 km i nie więcej niż 50 km

2. Architektura i konstrukcja.

- CPD musi zapewnić dostępność dedykowanych pomieszczeń serwisowych wraz z wyposażeniem stanowisk pracy (urządzenia pomiarowe i testowe, stoły elektrostatyczne, zasilanie 230V) nie mniej niż 2 stanowiskach pracy.
- Wysokość technologiczna Pomieszczeń Serwerowych (wysokość mierzona od podłogi technicznej do sufitu) nie mniejsza niż 350m.
-
- Wysokość podłogi technicznej nie mniejsza niż 100cm.
-
- Brak okien w Pomieszczeniach Serwerowych i Technicznych.
- Pomieszczenia Serwerowe i Techniczne muszą być pozbawione zbędnych instalacji stanowiących źródła zagrożeń, brak instalacji wodno-kanalizacyjnych, grzewczych)
- W Pomieszczeniu Serwerowym nie mogą występować słupy/podpory/filary lub inne pionowe elementy konstrukcyjne.
- Pomieszczenia Serwerowe i Techniczne muszą być wykonane w całości w technologii konstrukcji betonowej.
-
- Odporność ogniowa stropów i ścian Pomieszczeń Serwerowych i Technicznych. Nie gorszy niż B60.
- Odporność ogniowa drzwi Pomieszczeń Serwerowych i Technicznych. Nie mniejszy niż EI 60.

- Minimalna odległość Pomieszczeń Serwerowych od źródeł pól zakłócających (transformatory SN i WN). Wiecej niż 15m.

3. ZASILANIE

- Infrastruktura zasilania CPD musi zapewniać redundancję energetyki zawodowej na poziomie trafo GPZ 110/15 kV,
- Wymagana ilość przyłączy SN (15 kV) nie mniej niż 2.
- Wymagana ilość niezależnych 2 torów zasilających NN w każdym Pomieszczeniu Serwerowym. Wszystkie tory zasilające muszą gwarantować taką samą moc maksymalną zasilania.
- Zasilanie do Szaf musi być prowadzone pod podłogą techniczną
- 3 faz każdego toru zasilającego w Pomieszczeniu Serwerowym
- Minimalna moc jednego PDU (Power Distribution Unit) 16 [kW].
- Minimalna ilość 2 PDU (Power Distribution Unit) w każdej Szafie .
- 6 Wyłączników nadprądowych S300 C, 16 A w każdym PDU
- Kontrola napięcia dla grupy gniazd w każdym PDU
- Poziom redundancji urządzeń UPS dla każdego toru zasilającego NN z osobna – 2N.
- CPD musi posiadać automatyczny system załączania rezerwy (SZR) zarówno po stronie SN
- CPD musi posiadać automatyczny system załączania rezerwy (SZR) zarówno po stronie NN.
- Każdy agregat prądotwórczy w CPD powinien znajdować się w zamkniętym Pomieszczeniu Technicznym o konstrukcji żelbetonowej odseparowanej od konstrukcji Pomieszczenia Serwerów
- Każdy agregat prądotwórczy w CPD powinien być wyposażony w specjalistyczne grzałki utrzymujące stałą temperaturę agregatu.
- Każdy agregat prądotwórczy w CPD powinien posiadać certyfikat producenta agregatu poświadczający jego przeznaczenie do pracy ciągłej.
- Oddzielny, dedykowany, redundantny system zasilania gwarantowanego dla zasilania szaf klimatyzacji precyzyjnej.
- Własna rozdzielnią średniego napięcia (SN) na Terenie.
- Gwarantowany czas podtrzymania zasilania przez system zasilaczy awaryjnych UPS nie mniej niż 15 minut przy pełnym obciążeniu elektrycznym Pomieszczenia Serwerowego
- Każdy agregat prądotwórczy w CPD posiada system dostarczania paliwa z zewnętrznym (minimum 20 tys. litrów) i dedykowanym wewnętrznym (znajdującym się w Pomieszczeniu Technicznym) zbiornikiem paliwa.
- Czas pracy każdego agregatu prądotwórczego w CPD gwarantujący zasilanie urządzeń w Pomieszczeniu Serwerowym, bez uzupełniania zbiorników, przez nie mniej niż 72h..
- System dostarczania paliwa do każdego agregatu prądotwórczego w CPD pozwala na tankowanie zbiornika podczas pracy agregatu.
- Gwarantowany czas dostawy paliwa. CPD posiada umowę z zewnętrznym dostawcą z gwarantowanym czasem dostawy.

4.SYSTEM PRZECIWOPOŻAROWY I WENTYLACJA CPD

- Pomieszczenia Serwerowe i Techniczne muszą posiadać system gaszenia gazem bezpiecznym dla sprzętu komputerowego i ludzi w postaci stałego urządzenia gaśniczego (SUG).

- System gaszenia w postaci stałego urządzenia gaśniczego (SUG) musi mieć możliwość powtórnego wyrzutu gazu w Pomieszczaniach Serwerowych i Technicznych z zapasowego zestawu butli z gazem.
- Czas przywrócenia gotowości system gaszenia w postaci stałego urządzenia gaśniczego (SUG) do powtórnego wyrzutu gazu (uruchomienie zapasowego zapasu butli) w Pomieszczaniach Serwerowych i Technicznych. Nie dłużej niż 5 min.
- Wymagany poziom natężenia dźwięku emitowanego przez dysze systemu gaszenia w postaci stałego urządzenia gaśniczego (SUG) w Pomieszczeniach Serwerowych. Nie więcej niż 100 dB.
- W Pomieszczeniach Serwerowych i Technicznych musi być stosowany czynnik gaśniczy systemu gaszenia w postaci stałego urządzenia gaśniczego (SUG), przystosowany do gaszenia urządzeń elektronicznych, nie powodujący korozji, nie pozostawiający żadnych osadów lub szkodliwych substancji w wyniku rozpadu cząsteczek czynnika.
- Minimalna wydajność instalacji wentylacji Pomieszczeń Serwerowych w celu przewietrzania po akcji gaszeniu (wymiana całej objętości powietrza) w Pomieszczeniach Serwerowych. Co najmniej 5 wymian na godzinę.
- Klasa filtracji powietrza przez system wentylacji do zapewnienia jakości powietrza wewnątrz Pomieszczeń Serwerowych. Nie gorsza niż G4.
- Współpraca systemu gaszenia w postaci stałego urządzenia gaśniczego (SUG) z systemem wczesnej detekcji dymu, oraz systemem BMS
- CPD musi gwarantować stosowanie działań prewencyjnych w zakresie wczesnego wykrywania zagrożeń pożarowych obejmujące monitorowanie Pomieszczeń Serwerowych za pomocą kamery termowizyjnej
- Pomieszczenia Serwerowe i Techniczne CPD muszą być wyposażone w system wczesnej detekcji dymu.
- Klasa detektorów systemu wczesnej detekcji dymu zgodnie z definicją ujętą w EN60950 (tzn. urządzenie jest przeznaczone do pracy przy zasilaniu z bezpiecznych niskich napięć i nie wytwarza żadnych napięć niebezpiecznych). Nie gorsza niż 11.
- Detektory systemu wczesnej detekcji dymu muszą spełniać wymagania zawarte w normie EN54-20 dotyczące klasy czułości A, B oraz C.
- Zakres czułości cząstek detektorów systemu wczesnej detekcji dymu Od 0,003 do 10 mikronów.
- Czułość systemu wczesnej detekcji dymu od 0,0015% do 25% (zadym/m).
- Ilość poziomów alarmów systemu wczesnej detekcji dymu nie mniej niż 4
- Funkcja detekcji dymu przez detektory systemu wczesnej detekcji dymu – rozróżnianie rodzaju pyłu
- System dostrajania progu czułości detektorów systemu wczesnej detekcji dymu w zależności od poziomu zanieczyszczenia tła (powietrza na zewnątrz CPD).
- Niezależne poziomy czułości pracy detektorów systemu wczesnej detekcji dymu w czasie dnia oraz w nocy.

5. SYSTEM KLIMATYZACJI PRECYZYJNEJ

- Redundantny układ produkcji i dystrybucji chłodu do Pomieszczeń Serwerowych N+1
- Redundancja dla elementów systemu klimatyzacji wewnątrz Pomieszczeń Serwerowych Nie gorsza niż N+1
- Czynnik chłodzący obiegu roztwór glikolu etylenowego

- Technologia wykonania rurarzu obiegów czynnika chłodzącego Polipropylen w wersji stabilizowanej włóknem szklanym
- System klimatyzacji umożliwia wymianę ciepłą z otoczeniem w tzw. „free-coolingu" z wykorzystaniem glikolu jako nośnika chłodu
- Redundancja rurarzu obiegów czynnika chłodzącego nie gorsza niż 2N
- Sterowanie parametrami pracy wszystkich elementów systemu przez system BMS
- Pomieszczenie Serwerowe musi zapewniać separację stref zimnych/ciepłych
- Nawiew zimnego powietrza musi odbywać się pod podłogą techniczną
- Temperatura w zamkniętej strefie zimnej Pomieszczenia Serwerowego 25°C z tolerancją 5°C
- Wilgotność względna w zamkniętej strefie zimnej Pomieszczenia Serwerowego 55% z tolerancją 15%
- Maksymalna zmiana temperatury w zamkniętej strefie zimnej Pomieszczenia Serwerowego Nie więcej niż5°C/godzina
- Maksymalna zmiana wilgotności w zamkniętej strefie zimnej Pomieszczenia Serwerowego Nie więcej niż 6 % /godzinę
- CPD musi zapewnić nieprzezierną separację Pomieszczeń Serwerowych od urządzeń systemu klimatyzacji.

6. SYSTEMY BEZPIECZEŃSTWA I ORGANIZACJA

- 7 stref bezpieczeństwa, rozumianych jako punkty autoryzacji i weryfikacji uprawnień do dostępu, od zewnątrz (z poza Terenu) do urządzeń w Pomieszczeń Serwerowych.
- Kontrola wejścia do CPD osób niezatrudnionych w CPD realizowana w oparciu o dokument tożsamości.
- Kontrola dostępu w CPD realizowana w oparciu o biometrię dla wejścia do wszystkich Pomieszczeń Serwerowych
- Kontrola dostępu do Pomieszczeń Serwerowych i Technicznych realizowana w oparciu o system RFID oraz kody dostępu.
- CPD musi posiadać umowę z koncesjonowaną agencją ochrony zatrudniającą koncesjonowanych pracowników ochrony mienia.
- CPD musi posiadać System Sygnalizacji Włamania i Napadu
- CPD musi posiadać instalację odgromową zgodnie z normami PN-IEC 61024 ,PN-EN 62305 Klasa I.
- CPD musi posiadać system telewizji przemysłowej (CCTV)
- System telewizji przemysłowej (CCTV)w CPD musi zapewnić monitoring wszystkich ciągów komunikacyjnych
- System telewizji przemysłowej (CCTV)w CPD musi być wyposażony w kamery cyfrowe o minimalnej wymaganej jakości obrazu. Nie mniej niż 1,3Mpix. Nie mniej niż 8 ramek/s
- System telewizji przemysłowej (CCTV)w CPD musi posiadać funkcję detekcji ruchu,
- Czas archiwizacji zapisu obrazów z kamer systemu telewizji przemysłowej (CCTV) w CPD nie mniej niż 90 dni
- CPD musi zapewnić ciagłą obserwację wszystkich drzwi, okien, włazów, otoczenia budynku.
- Obiekt CPD musi posiadać obszary chronione system alarmowym zgodnym z normą PN-93/E-08390 na poziomie minimum SA3
- Pomieszczenia Serwerowe w CPD muszą być wyposażone w system wykrywania wody na powierzchni technicznej (podłodze) przy klimatyzatorach i innych instalacjach wodnych

7. SIEĆ

- Ilość niezależnych przyłączy światłowodowych traktowany jako niezależny rurarz/kanalizacja teletechniczna. Nie mniej niż 2 (dla każdego ośrodka).
- Każda z tras światłowodowych musi wychodzić z CPD w różnych kierunkach z wykorzystaniem niezależnej kanalizacji teletechnicznej
- Ilość niezależnych Pomieszczeń Technicznych będących punktami dystrybucji łącz teletechnicznych. Nie mniej niż 2.
- Ilość operatorów telekomunikacyjnych, innych niż operator CDP, posiadających własne światłowodowe kable telekomunikacyjne do CPD traktowane jako przyłącza światłowodowe minimum 12 włókien poprowadzone od własnej sieci do CPD. Nie mniej niż 2 (dla każdego ośrodka)
- 3 operatorów posiadających w CPD węzeł dostępowy do sieci Internet
- Ośrodki powinny być połączone minimum dwoma kablami światłowodowymi nx2J poprowadzonymi niezależnymi drogami. Światłowody nie mogą się przecinać w żadnym punkcie oraz nie mogą być zakończone w tym samym punkcie wymiany ruchu między operatorskiego.
- Operator Data Cener powinien być wyłącznym właścicielem kabli światłowodowych. Warunek spełniony dla minimum jednego kabla w ramach jednej drogi światłowodowej. Dopuszcza się by druga droga była zapewniona przez operatora data center na bazie umowy dzierżawy włókien światłowodowych w kablu operatora telekomunikacyjnego. Umowy dzierżawy z operatorem telekomunikacyjnym, jednak umowa dzierżawy musi obejmować okres dłuższy niż okres umowy z Zamawiającym. Operator data center powinien udokumentować akt wyłącznej własności kabla/kabli światłowodowych oraz (jeżeli zastosuje wariant dzierżawy) Operator data center powinien udokumentować akt wyłącznej dzierżawy włókien światłowodowych.
- CPD powinno być wyposażone w redundantny węzeł dostępu do sieci Internet z wykorzystaniem routerów, switchy, firewall, Intrusion Prevention System.
- CPD powinno posiadać zabezpieczenie przed atakami DDoS zainstalowane bezpośrednio w węźle operatora telekomunikacyjnego zapewniającą mitygację (czyszczenie ruchu) na poziomie nie mniejszym niż 10Gbps. Operator telekomunikacyjny który zapewnia ochronę DDoS powinien być osobnym podmiotem gospodarczym, odrębnym od operatora date center, nie powiązanym kapitałowo. Operator data center powinien udokumentować posiadanie zabezpieczenia DDoS (załączając wyciąg z umowy z operatorem telekomunikacyjnym).
- CPD musi posiadać własna publiczna adresacja IP.

8.SZAFY

- Kontrola dostępu do strefy zimnej realizowana w oparciu o system RFID oraz kody dostępu
- Każda szafa musi być wyposażona w system kontroli dostępu w postaci sterowanego i monitorowanego przez BMS elektrozaczepu.
- CPD musi zapewnić monitoring i logowanie otwarć drzwi w każdej szafie. Minimalny czas gromadzenia tych danych. Nie mniej niż rok.
- 2 elementy dystrybucji zasilania infrastruktury IT (PDU)
- Każdy element dystrybucji zasilania (PDU) w Szafie połączony z innym torem zasilającym

9.BMS

- CPD musi być wyposażone w dedykowany system Building Management System BMS
- System BMS CPD musi być oparty na programowalnych dedykowanych sterownikach logicznych (PLC)
- Sterowniki systemu BMS działają niezależnie od siebie tzn. że awaria jednego z nich nie ma wpływu na pracę pozostałych.
- System BMS w CPD musi zapewniać współpracę z urządzeniami typu switch/ruter IP
- Sterowniki systemu BMS zapewniają obsługę portów szeregowych RS232, RS422, RS485
- Sterowniki systemu BMS zapewniają kompatybilność z protokołem MODBUS
- Integracja systemu BMS z systemem zasilania umożliwiająca ciągły monitoring zasilania (obecność napięcia dla każdej fazy, wartość prądu, symetria faz) dla każdego PDU w każdej Szafie w Pomieszczeniu serwerowym
- Integracja systemu BMS z systemem klimatyzacji precyzyjnej umożliwiającą kontrolę parametrów powietrza powracającego do urządzeń klimatyzacji wewnątrz Pomieszczeń Serwerowych.
- System BMS w CPD musi zapewnić monitoring parametrów systemu generacji energii elektrycznej (min. tryb pracy i temperaturę każdego agregatu prądotwórczego w CPD).
- System BMS w CPD musi zapewnić monitoring SZR SN obejmujący tryby pracy, stan , obecność napięcia na linii podstawowej i rezerwowej.
- System BMS w CPD musi zapewnić monitoring SZR NN obejmujący tryby pracy, stan, obecność napięcia na linii podstawowej i rezerwowej.
- System BMS w CPD musi zapewnić monitoring UPS-ów (parametry elektryczne, alarmy, czas pracy na baterii, stan)
- System BMS w CPD musi zapewnić monitoring parametrów środowiskowych (temperatura, wilgotność, czujniki zalania).
- System BMS w CPD musi zapewnić monitoring pracy szaf klimatyzacji precyzyjnej.

III. Wymagania dotyczące Oferentów.

- Aktualny Certyfikat ISO 9001
- Aktualny Certyfikat ISO 27001
- Aktualny Certyfikat ISO 27017
- Personel obsługujący Data Center dostępny na miejscu
- Zespół inżynierów systemowych i sieciowych pracujących na miejscu
- Na miejscu aktywny departament ds. jakości i bezpieczeństwa
- Dedykowany portal do zgłaszania problemów i zleceń (system ticketowy)

Zamawiający zastrzega sobie prawo do wizyty weryfikacyjnej w ośrodku podstawowym i zapasowym. Zamawiającego celem weryfikacji spełnienia wymagań ZO. Wizyta taka może się odbyć na życzenie Zamawiającego w okresie pomiędzy złożeniem ofert a wyborem Wykonawcy. W przypadku niespełnienia któregokolwiek z wymaganych parametrów będzie skutkować odrzuceniem badanej oferty.