**Załącznik nr B7C – Cyberbezpieczeństwo OT– Infrastruktura sprzętowa (serwery, macierze, stacje robocze, stacje inżynierskie, tablety wzmacniane, KVM,** **komponenty infrastrukturalne środowiska wirtualnego,** **komponenty infrastrukturalne kontrolera domeny OT, Urządzenie do backupu dyskowego z deduplikacją) OT**

**Program Funkcjonalno- Użytkowy**

Spis treści

[1 Standard w zakresie umów serwisowych 3](#_Toc184642316)

[1.1 Wymagania ogólne dostarczanych urządzeń: 3](#_Toc184642317)

[1.2 Wymagany poziom serwisu (wymagania minimalne): 4](#_Toc184642318)

[2 Infrastruktura sprzętowa (serwery, macierze, KVM) OT 5](#_Toc184642319)

[2.1 Wirtualizacja serwerów 5](#_Toc184642320)

[2.2 Wirtualizacja Macierzy dyskowych 5](#_Toc184642321)

[2.3 Serwery 6](#_Toc184642322)

[2.4 Macierze dyskowe 6](#_Toc184642323)

[2.5 KVM – specyfikacja techniczna 6](#_Toc184642324)

[2.6 Monitory 6](#_Toc184642325)

[2.7 Instalacja minimalnej ilości ,,pakietów” systemu operacyjnego lub serwisów 7](#_Toc184642326)

[2.8 Poprawki bezpieczeństwa 7](#_Toc184642327)

[2.9 Dostęp administracyjny 7](#_Toc184642328)

[2.10 Zbędne usługi sieciowe, protokoły i funkcje 8](#_Toc184642329)

[2.11 Konfiguracja wewnętrznej zapory ogniowej 8](#_Toc184642330)

[2.12 Uprawnienia do plików 8](#_Toc184642331)

[2.13 Polityka dla kont i haseł 9](#_Toc184642332)

[2.14 Bazy danych 9](#_Toc184642333)

[3 Infrastruktura sprzętowa (stacje operatorskie, stacje inżynierskie) OT. 9](#_Toc184642334)

[3.1 Wymagania odnośnie stacji operatorskich. Ze względu na standaryzację w GK PGE dopuszcza się stacje operatorskie i inżynierskie producentów Dell oraz HP. 9](#_Toc184642335)

[4 Infrastruktura sprzętowa (komponenty infrastrukturalne środowiska wirtualnego) 10](#_Toc184642336)

[4.1 Wymagana specyfikacja sprzętowa infrastruktury serwerowej dla środowiska wirtualnego. 10](#_Toc184642337)

[5 Infrastruktura sprzętowa (komponenty infrastrukturalne kontrolera domeny OT) 11](#_Toc184642338)

[5.1 Wymagana specyfikacja infrastruktury serwerowej dla kontrolera domeny. 11](#_Toc184642339)

[6 Insfrastruktura sprzętowa (Urządzenie do backupu dyskowego z deduplikacją) 12](#_Toc184642340)

[6.1 Specyfikacja wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej 12](#_Toc184642341)

1. Standard w zakresie umów serwisowych

## Wymagania ogólne dostarczanych urządzeń:

* 1. Wszystkie urządzenia musza być fabrycznie nowe i pochodzić z seryjnej produkcji (tzn. wyprodukowane nie dawniej niż na 6 miesięcy przed ich dostarczeniem). Ponadto Zamawiający wymaga, aby dostarczane urządzenia nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest on zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).
  2. Wszystkie elementy dostawy powinny być jednoznacznie opisane w ofercie tj. zawierać odpowiednią nazwę części/ elementu/ licencji wraz z numerem produktu umożliwiającym jednoznaczną identyfikację.
  3. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
  4. Przy dostawie wymagane jest dostarczenie wykazu wszystkich oferowanych części i licencji wraz z ich oznaczeniami Part Number oraz Serial Number. Przed podpisaniem protokołu odbioru Zamawiający zastrzega sobie prawo do weryfikacji u producenta, czy dostarczony sprzęt oraz oprogramowanie pochodzi z autoryzowanego źródła oraz czy serwis gwarancyjny na wszystkie elementy dostawy będzie świadczony przez producenta na warunkach i w okresie zgodnym z wymaganiami określonymi przez Zamawiającego w niniejszej specyfikacji.
  5. Przy dostawie wymagane jest dostarczenie wykazu wszystkich oferowanych części i licencji wraz z ich oznaczeniami Part Number oraz Serial Number. Przed podpisaniem protokołu odbioru Zamawiający zastrzega sobie prawo do weryfikacji u producenta, czy dostarczony sprzęt oraz oprogramowanie pochodzi z autoryzowanego źródła oraz czy serwis gwarancyjny na wszystkie elementy dostawy będzie świadczony przez producenta na warunkach i w okresie zgodnym z wymaganiami określonymi przez Zamawiającego w niniejszej specyfikacji.
  6. Urządzenia i ich komponenty muszą być wolne od wad fizycznych i prawnych oraz nie może toczyć się żadne postępowanie, którego przedmiotem są zamawiane Urządzenia i ich komponenty, jak również nie mogą być one obciążone zastawem, zastawem rejestrowym, ani zastawem skarbowym, ani żadnymi innymi ograniczonymi prawami rzeczowymi.
  7. Zamawiający wymaga, by oferowane oprogramowanie było oprogramowaniem w wersji najaktualniejszej stabilnej i rekomendowanej przez Wykonawcę na dzień montażu.
  8. Wykonawca musi dołączyć do oferty specyfikację techniczną oferowanego rozwiązania wydaną przez producenta urządzenia potwierdzającą spełnienie stawianych wymagań. Wykonawca ma podać w ofercie adres strony www producenta sprzętu, na której jest dostępna ww. specyfikacja techniczna (dopuszcza się dokumenty w języku angielskim).
  9. Przy zastrzeżeniu zapisów pkt 1 urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
  10. Zamawiający wymaga dostępu do ogólnopolskiej infolinii/linii technicznej z każdej lokalizacji, w której będzie realizowany przedmiot zamówienia, dla dostarczonych urządzeń w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. Zamawiający dopuszcza realizację powyższych wymagań za pośrednictwem strony www producenta urządzeń.
  11. Urządzenia muszą pochodzić z autoryzowanego przez producenta sprzętu kanału sprzedaży na terenie Unii Europejskiej, a gwarancja musi być świadczona przez sieć serwisową dostępną na terenie Polski w oparciu o oryginalne materiały i części dostarczane przez producenta i zgodnie z jego zaleceniami.
  12. Zamawiający wymaga, aby przed podpisaniem Protokołu Odbioru sprzętu i oprogramowania Wykonawca przedstawił na życzenie Zamawiającego oficjalne potwierdzenie wykupienia kontraktów serwisowych u Producenta, a jeżeli jest to niemożliwe to przedstawił oświadczenie o posiadaniu aktualnych kontraktów serwisowych, na dostarczone urządzenia i oprogramowanie zgodnie z warunkami Umowy.
  13. Wszystkie urządzenia muszą posiadać deklaracje zgodności CE produktu. Przed podpisaniem Protokołu Odbioru sprzętu, Wykonawca na życzenie Zamawiającego przedstawi deklaracje zgodności CE produktów.
  14. Jeżeli dla spełnienia warunków gwarancji wymagane są okresowe przeglądy i konserwacja urządzeń, Wykonawca realizuje je na własny koszt.
  15. Wykonawca zobowiązany jest do poniesienia wszelkich kosztów związanych z naprawą gwarancyjną, w tym koszty transportu.
  16. Warunki serwisu nie mogą nakładać na Zamawiającego konieczności przechowywania oryginalnych opakowań po sprzęcie. W przypadku, gdy w ramach zgłoszenia serwisowego wymagane jest oryginalne opakowanie, dostarczenie takiego opakowania leży po stronie Wykonawcy. Zamawiający nie przechowuje opakowań po dostarczonych urządzeniach.
  17. O ile w treści specyfikacji występują wkładki do portów urządzeń sieciowych to powinny one pochodzić z oferty producenta zaoferowanych urządzeń sieciowych.
  18. Zamawiający wymaga dostępności części zamiennych oraz wsparcia na sprzęt i licencje do czasu zakończenia okresu gwarancyjnego na System.
  19. Zamawiający wymaga fizycznej instalacji oferowanych urządzeń w uzgodnionej lokalizacji (we wskazanej szafie) oraz wykonania testów uruchomieniowych. Lokalizacja może znajdować się na kondygnacji budynku – koszty wniesienia oraz montażu urządzeń ponosi Wykonawca.

## Wymagany poziom serwisu (wymagania minimalne):

* 1. W okresie gwarancyjnym wymagane jest dla wszystkich elementów infrastruktury OT wsparcie pozwalające na wykonywanie zgłoszeń 24/7/365.
  2. Elementy sprzętowe muszą być objęte wsparciem z gwarantowanym czasem naprawy on-site.
  3. Oprogramowanie musi zostać objęte opieką Producenta z gwarancją dostępu do wszystkich najnowszych wersji oprogramowania, w tym nowych wersji głównych (update i upgrade),
  4. Od Dostawców rozwiązań wymagane jest udzielenie minimum 60 miesięcznej gwarancji na wdrożenie, konfigurację i elementy środowiska z gwarantowanym czasem naprawy on-site.
  5. gwarancja producenta urządzeń - 60 miesięcy od momentu podpisania protokołu odbioru.
  6. Czas usunięcia awarii – 24 godziny zegarowe od momentu uzyskania dostępu do urządzenia i przyjęcia zgłoszenia serwisowego przez Zamawiającego.
  7. W przypadku macierzy dyskowych wymaganym poziomem wsparcia jest NBD (Next Business Day) wraz opcją pozostawienia dysków u Zamawiającego.
  8. Naprawa musi być wykonywana w miejscu instalacji urządzenia (dopuszczalne jest wykonanie zdalnej diagnostyki przed usunięciem awarii).
  9. Deklaracja realizacji napraw w czasie 24 godzin od momentu zgłoszenia awarii jest jednoznaczna z obligatoryjnym posiadaniem przez Wykonawcę sprzętu zastępczego dedykowanego do obsługi napraw u Zamawiającego.
  10. W przypadku nie dotrzymania warunków serwisowych Zamawiający zastrzega sobie prawo realizacji naprawy w wybranym serwisie i obciążenia Wykonawcy kosztami.
  11. Zamawiający wymaga prawa do pobrania, użytkowania oraz instalacji nowych wersji oprogramowania systemowego (również wnoszących nowe funkcjonalności) w całym okresie trwania gwarancji.
  12. W przypadku stwierdzenia błędów krytycznych w oprogramowaniu systemowym dla dostarczonych urządzeń, Wykonawca zobowiązany jest do usunięcia tych błędów nieodpłatnie, poprzez wymianę wersji oprogramowania systemowego, do wersji rekomendowanej przez producenta w ramach posiadanych przez Zamawiającego funkcjonalności urządzenia i oprogramowania w całym okresie trwania gwarancji.
  13. Wszelkie zmiany w konfiguracji wymagane dla zmiany oprogramowania usuwającego błędy krytyczne w urządzeniach muszą być wykonane przez Wykonawcę.

1. Infrastruktura sprzętowa (serwery, macierze, KVM) OT

## Wirtualizacja serwerów

1. Na wszystkich serwerach wirtualnych instalowanych na platformie VMware mają być instalowane VMware Tools zgodne z wersją ESXi.
2. Platformy wirtualizacyjne są zarządzane z jednego centralnego punktu (np. vCenter dla VMware)
3. Wirtualizacja jest rekomendowanym sposobem wdrażania serwerów aplikacyjnych.
4. Serwery fizyczne (hosty), jeśli używane są na potrzeby więcej niż jednego systemu lub aplikacji, powinny być dzielone z użyciem narzędzia puli zasobów zgodnie z wymaganiami aplikacji i systemów na nich uruchamianych.
5. Licencje VMware vSphere dla hostów muszą być dobrane zgodnie z ilością core, przy założeniu wykorzystania 70% zainstalowanej pamięci RAM. Poziom licencji vSphere musi być nie niższy niż EnterprisePlus
6. Wszystkie nowe licencje WMware vSphere muszą posiadać opcję Operations Management umożliwiającą rozszerzone możliwości zarządzania i monitorowania platformy wirtualizacyjnej.
7. Dobór ilości licencji na produkty instalowane na serwerach wirtualnych muszą uwzględniać zapisy licencyjne ich producentów co do stosowania na platformach wirtualizacyjnych.

## Wirtualizacja Macierzy dyskowych

1. Wymaga się wirtualizacji macierzy dyskowych, rekomenduje się zastosowanie rozwiązań typu VMware vSAN do współdzielenia przestrzeni dyskowej.

## Serwery

1. Wymagane jest aby serwery posiadały zdalny interfejs zarządzający dostępny poprzez sieć TCP/IP zapewniający integralność i poufność sesji.
2. Wymagane jest aby wraz z serwerami dostarczane oraz instalowane było oprogramowanie do zarządzania wraz z niezbędnymi licencjami.
3. Wymagane jest aby serwery miały możliwość zdalnego przejmowania konsoli w trybie tekstowym jak i graficznym.
4. Wymagane jest aby serwery miały możliwość zdalnego włączenia/wyłączenia/restartu.
5. Wymagane jest aby serwery miały możliwość zdalnego montowania zasobów dyskowych/obrazów płyt.
6. Wymagane jest aby serwery były wyposażone w redundantne zasilacze zasilane z systemów napięcia gwarantowanego na napięcie zgodne z warunkami obiektu i przeznaczeniem (systemy przemysłowe i telekomunikacyjne).
7. Wymagane jest aby serwery posiadały redundantne ścieżki boot’ujące w przypadku „boot from SAN” oraz redundantne dyski wraz z kontrolerem RAID w przypadku dysków lokalnych (w budowanych w serwer) wewnętrznych. Nie dopuszcza się stosowania kart SD jako nośników systemów operacyjnych w serwerach OT.
8. Wymagane jest, aby budowa serwerów umożliwiała szyfrowanie danych na dyskach wewnętrznych serwera.
9. Bezwzględnie wymaga się by interfejsy zarządzające serwerów podłączone były do oddzielnego, dedykowanego segmentu sieci LAN.
10. Zalecenia:
    * + Do specyficznych zastosowań (np. wysokowydajne serwery bazodanowe, serwery z potrzebą instalacji specjalistycznych kart przemysłowych) wymagane jest zastosowanie serwerów typu RACK.
      + Zalecane jest stosowanie wirtualizacji w zakresie interfejsów sieciowych LAN/SAN.

## Macierze dyskowe

1. Wymagane jest aby macierze posiadały zdalny interfejs zarządzający dostępny poprzez sieć TCP/IP zapewniający integralność i poufność sesji.
2. Wymagane jest aby macierze miały możliwość zdalnego włączenia/wyłączenia/restartu**.**
3. Wymagane jest aby macierze posiadały redundantne zasilacze zasilane z systemu napięcia gwarantowanego.
4. Wymagane jest aby macierze posiadały redundantne interfejsy zapewniające dostęp do danych.
5. Wymagane jest aby wraz z macierzami dostarczane oraz instalowane było oprogramowanie do zarządzania wraz z niezbędnymi licencjami.

## KVM – specyfikacja techniczna

1. Należy stosować KVM o następujących interfejsach minimalnych1 x HDMI i 4 x USB 2.0 Smart AVI,

## Monitory

1. Typ: LCD kolorowy o minimalnej przekątnej 26,5”
2. Rozdzielczość maksymalna nie mniejsza niż 1920x1080 na 60Hz,
3. Deklarowana jasność co najmniej 250 cd/m2
4. Deklarowany czas reakcji nie większy niż 8 ms (gray to gray)
5. Deklarowana ilość wyświetlanych kolorów nie mniejsza niż 16,7 mln
6. Monitor powinien zostać wyposażony w co najmniej dwa złącza sygnałowe:
   1. 1DisplayPort Wykonawca musi dostarczyć przewody umożliwiające podłączenie monitora z zaoferowanym złączem do komputera.
   2. HDMI lub DisplayPort lub VGA. Wykonawca musi dostarczyć przewody umożliwiające podłączenie monitora z zaoferowanym złączem do komputera. Dodatkowe złącza:
   3. 2 x USB 3.0 lub nowszy standard (HUB)
7. Minimum 2 głośniki zintegrowane z monitorem lub rozwiązanie producenta pozwalające zamontować trwale panel z głośnikami do obudowy monitora o mocy nie mniejszej niż 1 W każdy. W przypadku zastosowania drugiego wariantu dostawca zobowiązuje się dostarczyć monitory z takim panelem głośnikowym.
8. Obrotowa podstawka z regulacją wysokości w zakresie od 100 mm z możliwością obrotu ekranu pion/poziom oraz regulacją kąta pochylenia ekranu.
9. Zintegrowane z monitorem złącze umożliwiające podłączenie dodatkowo słuchawki lub słuchawek.

## Instalacja minimalnej ilości ,,pakietów” systemu operacyjnego lub serwisów

1. W systemie powinny istnieć wyłącznie pakiety, niezbędne do poprawnego funkcjonowania systemu operacyjnego oraz aplikacji, które będą działać w jego środowisku. Generalnie można przyjąć zasadę, że instalujemy system w wariancie minimalnym oraz dodajemy tylko niezbędne pakiety/funkcjonalności. Wyjątkiem są narzędzia diagnostyczne które są niezbędne przy diagnozowaniu problemów oraz rozwiazywaniu awarii (telnet, netcat, nc, traceroute, nslookup, dig, drill).

## Poprawki bezpieczeństwa

1. Oprogramowanie systemu operacyjnego oraz aplikacyjnego będzie posiadać zainstalowane wszystkie ostatnie stabilne poprawki bezpieczeństwa. Dotyczy to zarówno systemu operacyjnego jak również oprogramowania zainstalowanego w jego środowisku.

## Dostęp administracyjny

1. Trybem zdalnego dostępu jest terminal (tryb konsoli znakowej po połączeniu szyfrowanym SSH).
2. Zdalny dostęp administracyjny, powinien być on realizowany wyłącznie z wykorzystaniem bezpiecznych protokołów (SSH v2, HTTPS TLS 1.1 lub w wersji wyższej). Nie można wykorzystywać protokołów nie zapewniających poufności i integralności przesyłanych informacji. Nie dopuszcza się stosowania dodatkowych pluginów takich jak Java oraz silverlight. Rekomendowane jest stosowanie HTML 5.0.
3. Zastosować ograniczanie zdalnego dostępu na konto root do niezbędnego minimum (dostęp do konta root możliwy wyłącznie z konsoli serwera, a uzyskanie zdalnego dostępu na prawach użytkownika root, wymaga uprzedniego zalogowania się na konto indywidualne).
4. Czas wygasania nieaktywnych sesji użytkowników (nie dotyczy stacji operatorskich systemu nadrzędnego) musi być jak najkrótszy. Po upływie tego czasu powinno nastąpić rozłączenie sesji lub zablokowanie dostępu. Jeżeli system posiada możliwość włączenia wygaszacza ekranu zabezpieczonego hasłem, powinien się on aktywować po upływie 10 minut.
5. Użytkownikom logującym się do systemów operacyjnych powinien zostać wyświetlony komunikat ostrzegawczy, informujący o monitorowaniu prowadzonych działań i konsekwencjach działań nieuprawnionych. Wyświetlenie komunikatu powinno następować przed zalogowaniem się do systemu.
6. Należy stosować wyłączanie funkcjonalności wyświetlania identyfikatora użytkownika uprzednio zalogowanego do systemu, o ile system dysponuje taką możliwością.
7. Należy zastosować tak zwany port knocking, czyli włączania nasłuchiwania dla danej usługi dopiero po autoryzacji w inny sposób, na przykład otworzenie dostępu do zdalnego panelu zarządzania tylko dla naszego adresu IP dopiero po zalogowaniu się uprzednio w inne miejsce.
8. Aby uniknąć niepotrzebnych automatycznych prób zalogowania na serwerach wystawionych w sieci (na przykład na port ssh/22) należy przenieść taką usługę na wyższy port, na przyklad na 65422 gdzie bedzie ona ,,wolna” od automatycznych botów i narzędzi tak zwanych script kiddies.

## Zbędne usługi sieciowe, protokoły i funkcje

1. System nie powinien posiadać uruchomionych żadnych zbędnych usług sieciowych i udostępniać zbędnych protokołów i funkcji. Udostępnione elementy muszą mieć potwierdzenie w wymaganym przeznaczeniu systemu i aplikacji w nim działających.
2. Należy stosować oprogramowania typu PROXY dla usług sieciowych.

## Konfiguracja wewnętrznej zapory ogniowej

1. Jeżeli system posiada możliwość uruchomienia i skonfigurowania zapory ogniowej, powinna być ona włączona. Zapora powinna dopuszczać ruch wyłącznie z uprawnionych adresów (lub przedziału adresów) i wyłącznie do usług sieciowych, które są niezbędne do realizacji podstawowych funkcji biznesowych serwera oraz usług związanych z jego zarządzaniem. Zapora powinna zapewnić pełną kontrolę ruchu pakietów (statefull inspection), oraz kontrolować stan bitów protokołu TCP. Zaleca się stosowania serwera proxy działającego w warstwie 7 ISO do kontroli ruchu sieciowego.
2. Aby dodatkowo zapobiec atakom typu DoS (czyli Denial of Service) należy skonfigurować na zaporze maksymalna ilość pakietów jaka będzie przepuszczana dla danej usługi portu.

## Uprawnienia do plików

1. Dla programów, które posiadają ustalone bity SUID i SGID, a nie są wykorzystywane przez nieuprzywilejowanych użytkowników, należy je wyszukać i usunąć te uprawnienia.
2. Nie mogą istnieć pliki posiadające ustawione uprawnienia, pozwalające na ich modyfikację przez dowolnego użytkownika w systemie. Wszystkie tego typu pliki powinny być wyszukane i jeżeli nie ma żadnych przesłanek, aby takie uprawnienia musiały istnieć, należy je usunąć.
3. W systemie nie mogą istnieć pliki bez przypisanego właściciela i grupy. Wszystkie tego typu pliki muszą być wyszukane i należy im przypisać odpowiedniego użytkownika i grupę.
4. Uprawnienia do plików w systemie, w tym do narzędzi systemowych i zainstalowanych aplikacji muszą być ograniczone do niezbędnego minimum.

## Polityka dla kont i haseł

1. Wszystkie zbędne konta systemowe, które nie są aktywnie wykorzystywane lub są przeznaczone dla działań niewymagających interaktywnego logowania muszą być zablokowane. W systemie nie mogą również istnieć żadne konta z pustymi hasłami, wszystkie takie konta muszą być wyszukane i musi być dla nich ustalone hasło dostępowe. Musi być wyłączona możliwość logowania na konta z pustym hasłem.
2. wymaga się aby skonfigurować tak system klasy UNIX aby korzystał z nowszych i zaawansowanych funkcji hashujących.
3. Należy system klasy UNIX przekonfigurować aby pozwalały na hasła dłuższe niż 8 znaków.

## Bazy danych

1. Bazy danych należy instalować na serwerach fizycznych.
2. Dla baz produkcyjnych nie można stosować wersji bezpłatnych (typu express) ze względu na ograniczenia i brak wsparcia. Wydania baz danych (Standard, Enterprise, etc.) muszą być ściśle skorelowane z wymaganiami w zakresie funkcjonalności.
3. Infrastruktura sprzętowa (stacje operatorskie, stacje inżynierskie) OT.

## Wymagania odnośnie stacji operatorskich. Ze względu na standaryzację w GK PGE dopuszcza się stacje operatorskie i inżynierskie producentów Dell oraz HP.

* 1. Minimalne wymagania parametrów technicznych dla stacji operatorskich i inżynierskich są określone przez producenta danego systemu.
  2. Optymalne wymagania parametrów technicznych stacji operatorskich i inżynierskich firmy Dell– specyfikacja:
     1. Intel® Core™ i5-12600 vPro® dwunastej generacji (18 MB pamięci podręcznej, 6 rdzeni, 12 wątków, od 3,3 GHz do 4,8 GHz, 65 W)
     2. NVIDIA® Quadro T400, z 2 GB pamięci GDDR6,
     3. 32 GB, DDR5, 4800 MHz, bez funkcji ECC, pamięć dwukanałowa
     4. Dysk SSD M.2 2280 PCIe x4 czwartej generacji NVMe Class 40 o pojemności 512 GB
     5. 3-letnia usługa ProSupport Plus for Client z serwisem na miejscu w następnym dniu roboczym
     6. Bezprzewodowa klawiatura i mysz,
     7. 1 port USB 3.2 Type-C® z obsługą standardu generacji 2x2
     8. 1 port USB 3.2 drugiej generacji z funkcją PowerShare
     9. 2 port Ethernet RJ45
     10. 2 port USB 3.2 pierwszej generacji
     11. złącze PS/2 szeregowe
     12. HDMI 2.0b / DisplayPort 1.4a (HBR3)
     13. USB Type-C z trybem alternatywnym DisplayPort
     14. Zasilacz sieciowy 240 W AC, wtyk okrągły 7,4 mm
     15. 1x Windows LTSC
  3. a. Optymalne wymagania parametrów technicznych stacji operatorskich i inżynierskich firmy HP– specyfikacja:
     1. Intel® Core™ i5 12500 12. Generacji
     2. Odrębna karta graficzna NVIDIA® T400 (4 GB dedykowanej pamięci GDDR6)
     3. 32 GB pamięci DDR5
     4. Dysk SSD 512GB

1. 1 port USB 3.2 Type-C® z obsługą standardu generacji 2x2
2. 1 port USB 3.2 drugiej generacji z funkcją PowerShare
3. 2 port Ethernet RJ45
4. 2 port USB 3.2 pierwszej generacji
5. złącze PS/2 szeregowe
6. HDMI 2.0b / DisplayPort 1.4a (HBR3)
7. USB Type-C z trybem alternatywnym DisplayPort
8. Zasilacz sieciowy 240 W AC, wtyk okrągły 7,4 mm
9. 1x Windows LTSC
   1. Wszystkie odstępstwa dotyczące parametrów technicznych stacji operatorskich i inżynierskich musza być zaakceptowane przez przedstawicieli Zamawiającego (Departament Inżynierii oraz Departament Cyberbezpieczeństwa i ICT).
10. Infrastruktura sprzętowa (komponenty infrastrukturalne środowiska wirtualnego)

## Wymagana specyfikacja sprzętowa infrastruktury serwerowej dla środowiska wirtualnego.

1. Minimalne wymagania parametrów technicznych dla infrastruktury serwerowej dla środowiska wirtualnego są określone przez producenta danego systemu.
2. Optymalne wymagania parametrów technicznych infrastruktury serwerowej dla środowiska wirtualnego - Dell PowerEdge R650XS\_SPO lub HP DL360 Gen9 8SFF CTO Server – specyfikacja:
   * 1. 1x PowerEdge R650xs Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM
     2. 2x Intel Xeon Gold 6334, 3,6GHz, 8 rdzeni/16 wątków, 11,2GT/s, 18MB pamięci podręcznej, Turbo, HT(165W), DDR4-3200 1x 8x2.5 Front Storage
     3. 1x Konfiguracja riser nr 1, 1 gniazdo OCP 3.0 (x16) + 1 gniazdo x16 + 2 niskoprofilowe gniazda x8
     4. 1x PowerEdge R650xs x4 or x10 or x8 NVMe Shipping Material
     5. 2x 32GB pamięci RDIMM, 3200MT/s, w modułach dwubankowych
     6. 1x iDRAC9 Enterprise piętnastej generacji
     7. 2x 480GB SSD SATA 6Gb/s 512 2,5" dysk AG do różnych zastosowań wymieniany bez wyłączania systemu, 3 DWPD
     8. 4x 960GB 2,5" SED vSAS SSD 12Gb/s 512e dysk AG do różnych zastosowań wymieniany bez wyłączania systemu, 3DWPD
     9. 1x PERC H755 SAS Front
     10. 2x Radiator do procesora o mocy mniejszej niż 185W
     11. 1x Dwa nadmiarowe zasilacze (1+1) z możliwością wymiany bez wyłączania systemu, 1400W,tryb mieszany, NAF
     12. 1x Intel X710-T4L czteroportowa karta 10GbE BASE-T OCP 3.0
     13. 1x Broadcom 5719 czteroportowa karta sieciowa 1GbE BASE-T, PCIe, niskoprofilowa
     14. 1x Windows Server 2022 Standard,16 rdzeni, FI, bez nośnika, bez licencji CAL, wersja wielojęzyczna
     15. 1x 10 szt. licencji CAL urządzeń na system Windows Server 2022/2019 (Standard)
3. Pamięć masowa nie gorsza niż modularna macierz dyskowa HPE MSA 2052 lub PowerVault ME5012.
4. Zastosowanie rozwiązania typu Hypervisor lub inne podobne rozwiązania gwarantujące wysoką niezawodność działania maszyn wirtualnych (VCenter).
5. Wszystkie odstępstwa dotyczące parametrów technicznych infrastruktury serwerowej dla środowiska wirtualnego musza być zaakceptowane przez przedstawicieli Zamawiającego (Departament Inżynierii oraz Departament Cyberbezpieczeństwa i ICT).
6. Infrastruktura sprzętowa (komponenty infrastrukturalne kontrolera domeny OT)

## Wymagana specyfikacja infrastruktury serwerowej dla kontrolera domeny.

1. Minimalne wymagania parametrów technicznych dla infrastruktury serwerowej dla kontrolera domeny OT są określone przez producenta danego systemu.
2. Optymalne wymagania parametrów technicznych infrastruktury serwerowej dla kontrolera domeny OT - Dell PowerEdge R650XS\_SPO lub HP DL360 Gen9 8SFF CTO Server – specyfikacja:
   * 1. 1x PowerEdge R650xs Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM
     2. 2x Intel Xeon Gold 6334, 3,6GHz, 8 rdzeni/16 wątków, 11,2GT/s, 18MB pamięci podręcznej, Turbo, HT(165W), DDR4-3200 1x 8x2.5 Front Storage
     3. 1x Konfiguracja riser nr 1, 1 gniazdo OCP 3.0 (x16) + 1 gniazdo x16 + 2 niskoprofilowe gniazda x8
     4. 1x PowerEdge R650xs x4 or x10 or x8 NVMe Shipping Material
     5. 2x 32GB pamięci RDIMM, 3200MT/s, w modułach dwubankowych
     6. 1x iDRAC9 Enterprise piętnastej generacji
     7. 2x 480GB SSD SATA 6Gb/s 512 2,5" dysk AG do różnych zastosowań wymieniany bez wyłączania systemu, 3 DWPD
     8. 4x 960GB 2,5" SED vSAS SSD 12Gb/s 512e dysk AG do różnych zastosowań wymieniany bez wyłączania systemu, 3DWPD
     9. 1x PERC H755 SAS Front
     10. 2x Radiator do procesora o mocy mniejszej niż 185W
     11. 1x Dwa nadmiarowe zasilacze (1+1) z możliwością wymiany bez wyłączania systemu, 1400W,tryb mieszany, NAF
     12. 1x Intel X710-T4L czteroportowa karta 10GbE BASE-T OCP 3.0
     13. 1x Broadcom 5719 czteroportowa karta sieciowa 1GbE BASE-T, PCIe, niskoprofilowa
     14. 1x Windows Server 2022 Standard,16 rdzeni, FI, bez nośnika, bez licencji CAL, wersja wielojęzyczna
     15. 1x 10 szt. licencji CAL urządzeń na system Windows Server 2022/2019 (Standard)
3. Wszystkie odstępstwa dotyczące parametrów technicznych infrastruktury serwerowej dla kontrolera domeny OT musza być zaakceptowane przez przedstawicieli Zamawiającego (Departament Inżynierii oraz Departament Cyberbezpieczeństwa i ICT).
4. Insfrastruktura sprzętowa (Urządzenie do backupu dyskowego z deduplikacją)

## Specyfikacja wymagań dla serwera do instalacji w infrastrukturze serwerowo-sieciowej

1. Minimalne wymagania parametrów technicznych dla infrastruktury serwerowo-sieciowej są określone przez producenta danego systemu.
2. Optymalne wymagania parametrów technicznych infrastruktury serwerowo-sieciowej - Veritas NetBackup 5250 lub HP StoreOnce 5200 36 TB – specyfikacja:
3. Urządzenie musi być kompletnym rozwiązaniem sprzętowym typu „appliance”. Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych.
4. Urządzenie musi oferować minimum 360 TiB przestrzeni użytkowej dla danych (bez deduplikacji).
5. Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii minimum RAID-6.
6. Urządzenie musi posiadać zapasowe dyski spare, które będą automatycznie włączane do grup RAID w przypadku awarii jednego z dysków produkcyjnych. Urządzenie musi posiadać co najmniej 1 dysk hot-spare na każde 20 dysków produkcyjnych.
7. Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie z standardem NIST SP 800-88 poprzez mechanizm wielokrotnego nadpisania przeterminowanych danych.
8. Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID.
9. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie.
10. Urządzenie musi umożliwiać rozbudowę pojemności użytkowej dla danych (bez deduplikacji) do co najmniej 780 TiB bez uwzględniania mechanizmów protekcji. Rozbudowa pojemności nie może wymuszać rozbudowy lub wymiany kontrolerów urządzenia – rozbudowa musi odbywać się jedynie poprzez instalację nowych dysków i/lub półek dyskowych.
11. Urządzenie musi posiadać dla ruchu produkcyjnego minimum:
    1. 4 porty FC 16 Gb/s z możliwością obsługi każdym portem FC protokołów VTL oraz deduplikacji na źródle,
    2. 4 porty Ethernet 10/25 Gb/s SFP z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle.
12. Do zarządzania musi posiadać minimum 2 porty Ethernet 1 Gb/s z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle,
13. Oferowane urządzenie musi posiadać możliwość obsługi do 8 portów FC 32 Gb/s lub 8 portów Ethernet 10/25 Gb/s lub dowolnej ich kombinacji.
14. Urządzenie musi osiągać w maksymalnej konfiguracji zagregowaną wydajność backupu protokołami CIFS/NFS/ VTL co najmniej 22 TB/h (dane podawane przez producenta) oraz co najmniej 41 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta), a także zagregowaną wydajność odtwarzania protokołami CIFS / NFS / VTL co najmniej 18 TB/h (dane podawane przez producenta).
15. Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.
16. Urządzenie musi pozwalać na jednoczesną obsługę minimum 500 strumieni (zapis danych, odczyt danych, replikacja danych).
17. Urządzenie musi umożliwiać podział na minimum 60 partycji logicznych w taki sposób, aby każdy z podłączonych systemów backupowych mógł pracować na osobnym urządzeniu logicznym. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
18. Urządzenie musi deduplikować dane inline przed zapisem na nośnik dyskowy. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości.
19. Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej).
20. Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane.
21. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
22. Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256
23. Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.
24. Urządzenie musi posiadać redundantne zasilacze i wentylatory.
25. Wszystkie odstępstwa dotyczące parametrów technicznych infrastruktury serwerowo-sieciowej musza być zaakceptowane przez przedstawicieli Zamawiającego (Departament Inżynierii oraz Departament Cyberbezpieczeństwa i ICT).