UMOWA 2020/INF/……..

zawarta w dniu ……. w Nysie pomiędzy:

Gminą Nysa, ul. Kolejowa 15, 48-300 Nysa, NIP: 7532414579, REGON 531412869, zwaną dalej „Zamawiającym" reprezentowanym przez:

- Kordiana Kolbiarza - Burmistrza Nysy,

a:

……..

……..

……..,

zwanym dalej „Wykonawcą" reprezentowanym przez:

……

……

……

Umowa została zawarta w wyniku rozstrzygnięcia postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, zgodnie z ustawą z dnia 29 stycznia 2004r. - Prawo zamówień publicznych (Dz. U. z 2019r., poz. 1843 t.j.).

PRZEDMIOT UMOWY

§ 1

1. Przedmiotem umowy jest realizacja zadania: **Komputeryzacja (informatyzacja) Urzędu Miejskiego w Nysie - Modernizacja i rozbudowa systemu infrastruktury wirtualizacji danych oraz systemu backupu danych.**
2. Szczegółowy zakres przedmiotu umowy określa „Opis przedmiotu zamówienia", stanowiący załącznik nr 1 do umowy oraz oferta Wykonawcy stanowiąca integralną część niniejszej umowy.

TERMIN REALIACJI

§ 2

1. Rozpoczęcie realizacji przedmiotu umowy ustala się na dzień podpisania umowy, tj. ……..
2. Wykonawca zobowiązuje się do zrealizowania przedmiotu umowy w terminie do dnia ……..

ZOBOWIĄZANIA STRON

§ 3

1. Wykonawca oświadcza, iż posiada kwalifikacje i uprawnienia wymagane do prawidłowego wykonania przedmiotu umowy i zobowiązuje się do realizacji umowy z należytą starannością.
2. Wykonawca oświadcza, że:
    1) dysponuje wykwalifikowanymi pracownikami w zakresie wdrażania projektów informatycznych,
    2) dysponuje wykwalifikowanymi pracownikami do przeprowadzenia instalacji oraz konfiguracji urządzeń i oprogramowania,
    3) jest uprawniony do sprzedaży urządzeń i oprogramowania do wykonywania kopii bezpieczeństwa oraz udzielenia licencji na korzystanie z tego oprogramowania,
    4) dostarczony sprzęt i oprogramowanie nie zawiera żadnych wad fizycznych lub prawnych i jego jakość nie budzi żadnych zastrzeżeń.
3. Przy wykonywaniu umowy Wykonawca ponosi odpowiedzialność za:
    1) kompetentne, rzetelne i terminowe wykonanie przedmiotu umowy,
    2) wszelkie szkody wyrządzone w mieniu Zamawiającego przez Wykonawcę przy wykonywaniu w siedzibie Zamawiającego, objętych przedmiotem umowy, prac instalacyjnych i konfiguracyjnych.
4. Wykonawca zobowiązuje się zaplanować i wykonywać prace związane z realizacją niniejszej umowy w taki sposób, by nie spowodowały zakłóceń w pracy systemów teleinformatycznych Zamawiającego i nie uniemożliwiły ich użytkowania. Prace o podwyższonym poziomie ryzyka muszą być prowadzone poza godzinami pracy Urzędu Miejskiego w Nysie, w tym również w dni wolne od pracy.
5. Wykonawca zobowiązuje się wykonać przedmiot umowy własnymi siłami. Powierzenie wykonania części przedmiotu umowy innym wykonawcom wymaga uprzedniej pisemnej zgody Zamawiającego pod rygorem nieważności. W takim przypadku, Wykonawca ponosi odpowiedzialność za działania i zaniechania podwykonawców, którym powierzył wykonanie przedmiotu umowy, jak za własne działanie lub zaniechanie.
6. Zamawiający zobowiązuje się, w ustalonym wcześniej zakresie, do zapewnienia Wykonawcy warunków do sprawnej i zgodnej z zasadami wynikającymi z niniejszej umowy realizacji przedmiotu umowy.

ZASADY REALIZACJI PRZEDMIOTU UMOWY

§ 4

1. Wykonawca zobowiązuje się do dostarczania całości sprzętu, licencji i oprogramowania, będących przedmiotem umowy na swój koszt i ryzyko, własnym transportem pod wskazany przez Zamawiającego adres. Sprzęt spełniający wymagania Zamawiającego zostanie dostarczony wraz ze wszystkimi akcesoriami niezbędnymi do prawidłowej pracy przy spełnieniu wymagań Zamawiającego dotyczących jego konfiguracji.
2. Dostarczony w ramach realizacji umowy sprzęt, oprogramowanie i certyfikaty licencyjne będą pochodzić z oficjalnych kanałów sprzedaży poszczególnych producentów.

3. Wykonawca zobowiązuje się do:
    1) przygotowania projektu wykonawczego obejmującego zakres wykonywanych prac przez Wykonawcę,
    2) zorganizowania i przeprowadzenia instruktaży dla pracowników Zamawiającego,
    3) wykonania i przekazania Zamawiającemu dokumentacji związanej z realizacją zamówienia w formie elektronicznej na płycie CD/DVD lub nośniku USB z wykorzystaniem jednego lub kilku formatów zapisu plików:
        - MS Word (wersje ostateczne dokumentów oraz ich wersje robocze),
        - PDF (wersje ostateczne dokumentów),
        - MS Excel (zestawienia tabelaryczne),
        - JPG, GIF, PNG,
        - oraz innych za zgodą Zamawiającego.
4. Realizację przedmiotu umowy potwierdzi protokół odbioru stwierdzający kompletność, poprawność i zgodność z wymaganiami Zamawiającego. Protokół zostanie podpisany przez osoby upoważnione, reprezentujące Strony umowy – ze strony Zamawiającego osobą upoważnioną jest Naczelnik Wydziału Informatyki Urzędu Miejskiego w Nysie, ze strony Wykonawcy …….. Szczegółowe warunki dokonania odbioru końcowego zawiera załącznik nr 2 do umowy.
5. W razie stwierdzenia niezgodności w dostarczonym przedmiocie umowy, Zamawiający wyznaczy Wykonawcy termin na uzupełnienia braków lub usunięcia wad/usterek, z zastrzeżeniem, że stanowić to będzie realizację przedmiotu umowy na warunkach opóźnienia.
6. Po bezskutecznym upływie terminu, o którym mowa w ust. 5, Zamawiający ma prawo odstąpić od umowy.

WYNAGRODZENIE I PŁATNOŚĆ

§ 5

1. Za należyte wykonanie przedmiotu umowy Wykonawcy przysługuje wynagrodzenie w wysokości: …… zł brutto, słownie złotych: ……. w tym należny podatek VAT, według stawki obowiązującej w dniu wystawienia faktury w kwocie …….. zł.
2. Wynagrodzenie, o którym mowa w ust. 1, obejmuje wszystkie koszty Wykonawcy związane z wykonaniem przedmiotu umowy.

§ 6

1. Podstawą wystawienia faktury będzie podpisany bez zastrzeżeń przez obie strony protokół odbioru, o którym mowa w § 4 ust. 4.
2. Wynagrodzenie płatne będzie przelewem na rachunek bankowy Wykonawcy wskazany na fakturze w terminie 21 dni od daty doręczenia do siedziby Zamawiającego prawidłowo wystawionej faktury VAT wraz z kopią protokołu odbioru, przy czym za dzień zapłaty uważać się będzie dzień złożenia w banku Zamawiającego polecenia przelewu środków na konto Wykonawcy.

3. Jeżeli termin płatności wynikający z umowy jest rozbieżny z terminem płatności zamieszczonym na fakturze, to obowiązujący jest termin płatności wynikający z umowy.

KARY UMOWNE

§ 7

1. Odpowiedzialność z tytułu niewykonania lub nienależytego wykonania umowy Strony opierają na zasadzie kar umownych, płatnych w następujących przypadkach i w następującej wysokości:
    1) Wykonawca zobowiązany jest do zapłaty Zamawiającemu kary umownej w przypadku:
        a) opóźnienia w realizacji przedmiotu umowy w wysokości 0,5% wynagrodzenia brutto (§ 5 umowy), liczonej za każdy dzień opóźnienia,
        b) opóźnienia w usunięciu wad, w tym stwierdzonych w okresie gwarancji w wysokości 0,1% wynagrodzenia brutto (§ 5 umowy), liczonej za każdy dzień opóźnienia.
    2) Strona umowy, która ponosi odpowiedzialność za odstąpienie od umowy przez drugą stronę, zobowiązana jest do zapłaty Stronie odstępującej od umowy, kary umownej w wysokości 10% wynagrodzenia umownego brutto (§ 5 umowy).
2. Zamawiający ma prawo odstąpić od umowy w przypadku i terminie wskazanym w art. 145 ustawy „Prawo zamówień publicznych". Odstąpienie powyższe nie nakłada na Zamawiającego obowiązku zapłaty kary umownej, o której mowa w ust. 1 pkt 2.
3. Wykonawca wyraża zgodę na potrącanie kar umownych z należnego mu wynagrodzenia, bez konieczności odrębnego wzywania do zapłaty kar.
4. Zastrzeżenie kar umownych, określonych w ust. 1 nie wyłącza prawa dochodzenia przez Strony na zasadach ogólnych odszkodowania uzupełniającego przewyższającego wysokość zastrzeżonych kar umownych.

GWARANCJA I SERWIS

§ 8

1. Wykonawca udziela Zamawiającemu wsparcia technicznego producenta na dostarczony:
    1) sprzęt …… na okres ……. miesięcy,
    2) oprogramowanie …… na okres ……. miesięcy.

    liczonych od dnia podpisania protokołu odbioru końcowego, o który mowa w § 4 ust. 4.
2. W okresie trwania gwarancji Wykonawca będzie nieodpłatnie serwisował sprzęt i usuwał wszystkie awarie i usterki uniemożliwiające lub utrudniające ciągłą pracę sprzętu i oprogramowania, w terminie określonym w ust. 10.
3. Wykonawca gwarantuje, że sprzęt dostarczony w ramach umowy będzie sprzętem nowym, nieregenerowanym, nierefabrykowanym, nienaprawianym, nieużywanym (niedostarczanym) wcześniej w innych projektach, nie będzie sprzętem z zakończonych linii produktowych (end-of-life) oraz nie starszym niż 6 miesięcy od daty produkcji. Sprzęt oraz licencje nie mogą naruszać praw własności oraz praw niematerialnych osób trzecich.
4. Sprzęt, oprogramowanie oraz licencje dostarczone w ramach realizacji umowy będą pochodziły z oficjalnego kanału sprzedaży producenta na terenie Polski.

5. Wykonawca gwarantuje, że posiada autoryzację lub status partnerski producenta dostarczanego sprzętu oraz załącza potwierdzenie posiadania takiego statusu wystawione przez producenta.
6. Wykonawca gwarantuje działanie sprzętu i oprogramowania zgodnie z załączoną dokumentacją techniczną i użytkową.
7. Gwarancja nie może ograniczać praw Zamawiającego do instalowania i wymiany w zakupionym sprzęcie standardowych kart i urządzeń zgodnie z zasadami sztuki w tym zakresie.
8. Awarie oraz usterki będą zgłaszane przez Zamawiającego za pomocą telefonu lub poczty elektronicznej do siedziby Wykonawcy:
    1) nr telefonu Wykonawcy: …….
    2) adres poczty elektronicznej Wykonawcy: ……
9. Wykonawca zapewnia przyjmowanie zgłoszeń przez 5 dni roboczych (poniedziałek – piątek), w godzinach 8:00-16:00. Zgłoszenie zawierać będzie nr seryjny sprzętu, model (podstawowe parametry), lokalizację sprzętu (adres, nr pomieszczenia), dane osoby zgłaszającej, datę i godzinę sporządzenia zgłoszenia, opis awarii/usterki.
10. Wykonawca zobowiązuje się usunąć usterki i przywrócić pełną sprawność i funkcjonalność w terminie do 2 dni kalendarzowych od momentu zgłoszenia.
11. Działania serwisowe realizowane będą na miejscu u Zamawiającego lub zdalnie w godzinach pracy obowiązujących u Zamawiającego, a w wyjątkowych sytuacjach także poza godzinami pracy.
12. W przypadku, gdy po przeprowadzeniu diagnostyki awarii/usterki sprzętu, Wykonawca stwierdzi, że czas potrzebny do przywrócenia jego sprawności przekroczy gwarantowany okres, o którym mowa w ust. 10, Wykonawca dostarczy własnym transportem równoważny sprzęt zastępczy o tej samej funkcjonalności na czas naprawy i udostępni go Zamawiającemu. Po zakończeniu naprawy Wykonawca zainstaluje naprawione urządzenie lub dokona wymiany na nie gorsze co do modelu i funkcjonalności.
13. W okresie udzielonej gwarancji Wykonawca świadczyć będzie w godzinach pracy Zamawiającego telefonicznie oraz za pomocą poczty elektronicznej usługę typu „help-desk" w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań.
14. W ramach oferowanego serwisu Wykonawca zorganizuje i zapewni dostęp do serwisów on-line producenta sprzętu (uprzywilejowany dostęp przez dedykowane konto autoryzowane nazwą użytkownika i hasłem).

POSTANOWIENIA KOŃCOWE

§ 9

1. Wykonawca nie może przenieść wierzytelności wynikającej z niniejszej umowy na osobę trzecią bez zgody Zamawiającego, wyrażonej na piśmie pod rygorem nieważności.
2. Jeżeli okaże się, że do sprawnej realizacji umowy niezbędne jest dokonanie wzajemnych dodatkowych uzgodnień, Strony poczynią te uzgodnienia niezwłocznie.

3. Wykonawca zobowiązany jest do niezwłocznego informowania Zamawiającego o każdej zmianie adresu siedziby i o każdej innej zmianie w działalności Wykonawcy mogącej mieć wpływ na realizację umowy. W przypadku niedopełnienia tego obowiązku Wykonawcę będą obciążać ewentualne koszty mogące wyniknąć wskutek zaniechania.
4. W sprawach nieuregulowanych niniejsza umową zastosowanie mają przepisy Kodeksu cywilnego.
5. Wykonawca zobowiązuje się do utrzymania w tajemnicy wszelkich danych o Zamawiającym oraz innych informacji jakie uzyskał w związku z realizacją niniejszej umowy bez względu na sposób i formę ich utrwalenia i przekazania z wyjątkiem danych i informacji, które zgodnie z obowiązującymi przepisami mogą być ujawnione.
6. Wszelkie spory jakie mogą wyniknąć pomiędzy Stronami w związku z realizacją postanowień niniejszej umowy, będą rozwiązywane polubownie.
7. W razie braku możliwości polubownego załatwienia sporu w terminie dłuższym niż 30 dni, spór poddany zostanie rozstrzygnięciu sądu właściwego miejscowo dla siedziby Zamawiającego.
8. Wszelkie zmiany i uzupełnienia postanowień niniejszej umowy mogą nastąpić za zgoda obu stron wyrażoną na piśmie, pod rygorem nieważności dokonanych zmian.
9. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla Wykonawcy i Zamawiającego.
10. Integralną część umowy stanowi oferta Wykonawcy oraz załączniki nr 1 i 2, obejmujące:
    1) Opis przedmiotu zamówienia – załącznik nr 1,
    2) Warunki dokonania odbioru końcowego - załącznik nr 2.

Zamawiający: **Wykonawca:**

....

Kontrasygnata Skarbnika:

.....

Załącznik nr 1

do umowy nr 2020/INF/……
z dnia ……..

Opis przedmiotu zamówienia

I. Przedmiot zamówienia.

Przedmiotem zamówienia jest realizacja zadania: **Komputeryzacja (informatyzacja) Urzędu Miejskiego w Nysie - Modernizacja i rozbudowa systemu infrastruktury wirtualizacji danych oraz systemu backupu danych**, obejmująca w szczególności:

1. Dostawę, instalację, konfigurację i integrację w środowisku zamawiającego macierzy dyskowej.
2. Dostawę, instalację, konfigurację i integrację w środowisku zamawiającego serwerów klastra VMware.
3. Dostawę, instalację, konfigurację i integrację w środowisku zamawiającego serwera kopii zapasowych danych.
4. Dostawę, instalację, konfigurację i integrację w środowisku zamawiającego biblioteki taśmowej.
5. Dostawę, instalację, konfigurację i integrację w środowisku zamawiającego oprogramowania do wykonywania kopii zapasowych danych.
6. Rozbudowę posiadanej macierzy dyskowej.
7. Rozbudowę posiadanych serwerów.
8. Rozbudowę posiadanych licencji na oprogramowanie Microsoft.
9. Rozbudowę posiadanych licencji na oprogramowanie VMware.
10. Przeprowadzenie szkoleń w zakresie dostarczonego oprogramowania wykonywania kopii zapasowych.
11. Przeprowadzenie szkoleń w zakresie oprogramowania VMware.
12. Przedłużenie wsparcia serwisowego dla posiadanych licencji Vmware.
13. Opracowanie dokumentacji, szczegółowo opisującej elementy wdrożenia i konfiguracji.
14. Świadczenie usług wsparcia technicznego w zakresie wdrożonej infrastruktury.

W ramach realizacji zadania wykonana zostanie reorganizacja i rozbudowa infrastruktury teleinformatycznej Zamawiającego, polegająca na konfiguracji dwóch ośrodków przetwarzania danych: PDC (Primary Data Center) oraz DRC (Disaster Recovery Center). Ośrodki wykorzystywać będą posiadaną przez Zamawiającego infrastrukturę LAN oraz SAN, zlokalizowaną pomieszczeniach technicznych Urzędu Miejskiego w Nysie.

W obu ośrodkach (PDC oraz DRC) zostaną skonfigurowane oraz uruchomione klastry VMware z uwzględnieniem replikacji miedzy ośrodkami, w ramach dostępnych i posiadanych mechanizmów i zasobów.

Obecne Centrum Przetwarzania Danych (PDC), wyposażone zostanie w nową macierz dyskową, nowe serwery klastra VMware. Ośrodek DRC wyposażony zostanie w posiadane (i rozbudowane w ramach niniejszego zadania) serwery oraz macierz dyskową.

II. Macierz dyskowa – 1 sztuka.

Macierz dyskowa, rozumiana jest przez Zamawiającego jako zestaw kombinacji dysków twardych HDD oraz dysków elektronicznych SSD, kontrolowanych przez pojedynczą parę kontrolerów macierzowych, pracujących w układzie redundantnym active/active, bez korzystania z zewnętrznych połączeń kablowych pomiędzy kontrolerami oraz działające bez udziału dodatkowych urządzeń wirtualizujących zasoby dyskowe grupy urządzeń dyskowych.

Realizacja zadania uwzględnia m.in.:

1. Dostarczenie, montaż i instalację kompletnego urządzenia w szafie RACK Zamawiającego.
2. Podłączenie dostarczonej macierzy dyskowej do infrastruktury sieciowej LAN oraz SAN (dwa urządzenia HP 824 Base16) Zamawiającego z zachowaniem redundancji połączeń, z zachowaniem rekomendacji producenta. Dostarczona macierz zostanie podłączona w lokalizacji PDC, w miejsce obecnie użytkowanej przez Zamawiającego macierzy dyskowej, z uwzględnieniem migracji danych. Obecnie posiadana przez Zamawiającego macierz dyskowa (po rozbudowie) zostanie przeniesiona do lokalizacji DRC i wykorzystana na potrzeby infrastruktury DRC.
3. Rekonfigurację sieci SAN i LAN, zapewniającą dostęp do zasobów sieciowych Zamawiającego.
4. Konfigurację oprogramowania systemowego i jego aktualizację do najnowszej wersji, rekomendowanej przez producenta.
5. Dostarczenie kompletnego okablowania i licencji niezbędnych do uruchomienia urządzenia, zintegrowania ze środowiskiem informatycznym Zamawiającego, z zapewnieniem spełnienia wymaganych funkcjonalności.
6. Wszelkie czynności konfiguracyjne zapewniające prawidłowy dostęp do obecnych zasobów, które muszą zostać wykonane dodatkowo w środowisku Zamawiającego. Zamawiający wymaga, aby wszelkie czynności konfiguracyjne, które są działaniami pośrednimi w celu osiągnięcia wymaganej funkcjonalności, były wykonane w sposób zalecany przez producenta posiadanych oraz dostarczanych urządzeń i oprogramowania.
7. Wykonawca dostarczy kompletne okablowanie i/lub moduły i licencje niezbędne do uruchomienia macierzy i zintegrowania jej ze środowiskiem informatycznym Zamawiającego.

Specyfikacja macierzy dyskowej:

Element / cecha	Charakterystyka (wymagania minimalne)
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”.
Przestrzeń dyskowa	Macierz musi udostępniać minimum 22.5 TB przestrzeni RAW zbudowanej w oparciu o minimum 18 dysków w technologii SAS i prędkości obrotowej min. 10k obr/min. Macierz wyposażona w minimum 5 dysków SSD SAS 12Gb o łącznej przestrzeni RAW nie mniejszej niż 9 TB.

Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 240 dysków twardych.
Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i NL SAS. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. Komunikacja z dyskami 12Gb SAS.
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC 16Gb. Kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC i LAN.
Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 12GB pamięci Cache, 24 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.
Interfejsy do hostów	Macierz musi posiadać, co najmniej 8 portów FC 16Gb obsadzone wkładkami SFP SW 16 Gb/s.
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Wymaga się możliwości definiowania przynajmniej następujących poziomów dostępu do macierzy: • administrator – pełen dostęp, • monitor – możliwość odczytu konfiguracji.
Kreator konfiguracji	System zarzadzania powinien posiadać funkcjonalność kreatora konfiguracji uruchamianego w przypadku braku zdefiniowanych pul dyskowych i wolumenów, w przypadku braku zdefiniowanych powiadomień oraz braku wykrycia jakichkolwiek zadań wykonywanych na macierzy.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Możliwość tworzenia wolumenów logicznych o pojemności maksymalnej co najmniej 140TB. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie Thin Provisioning.

	Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 2 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.

	Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.
Gwarancja	3-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez 24 godziny na dobę. Czas reakcji to kolejny dzień roboczy. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. W przypadku awarii dyski pozostają u Zamawiającego.

III. Serwery klastra VMware – 2 sztuki.

Realizacja zadania uwzględnia m.in.:

1. Dostarczenie, montaż i instalacja kompletnych urządzeń w szafie RACK Zamawiającego.
2. Podłączenie dostarczonych serwerów klastra VMware do infrastruktury sieciowej LAN (dwa urządzenia Cisco 9300-48T) oraz SAN (dwa urządzenia HP 824 Base16) Zamawiającego z zachowaniem redundancji połączeń, z zachowaniem rekomendacji producenta. Dostarczone serwery zostaną podłączone w miejsce dotychczasowych serwerów w lokalizacji PDC, z uwzględnieniem migracji maszyn wirtualnych.
3. Rekonfigurację sieci SAN i LAN, zapewniającą dostęp do zasobów sieciowych Zamawiającego.
4. Konfigurację oprogramowania systemowego i jego aktualizacja do najnowszej wersji, rekomendowanej przez producenta.
5. Dostarczenie kompletnego okablowania i licencji niezbędnych do uruchomienia urządzeń, zintegrowania ich ze środowiskiem informatycznym Zamawiającego, z zapewnieniem spełnienia wymaganych funkcjonalności.

6. Wszelkie czynności konfiguracyjne zapewniające prawidłowy dostęp do obecnych zasobów, które muszą zostać wykonane dodatkowo w środowisku Zamawiającego. Zamawiający wymaga, aby wszelkie czynności konfiguracyjne, które są działaniami pośrednimi w celu osiągnięcia wymaganej funkcjonalności, były wykonane w sposób zalecany przez producenta posiadanych oraz dostarczanych urządzeń i oprogramowania.
7. Wykonawca dostarczy kompletne okablowanie i/lub moduły i licencje niezbędne do uruchomienia serwerów i zintegrowania ich ze środowiskiem informatycznym Zamawiającego.

Specyfikacja serwera klastra VMware:

Element / cecha	Charakterystyka (wymagania minimalne)
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). Serwer z możliwością wyposażenia w zamykany na klucz, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. Serwer z możliwością fabrycznego zamontowania czujnika otwarcia obudowy współpracującego z modułem zarządzania serwera.
Procesor	Dwa procesory 12-rdzeniowe, x86 - 64 bity, Intel Xeon Gold 6226 (2.7GHz/12-core/125W) lub równoważne procesory dwunastordzeniowe, osiągające w testach SPECrate2017_int_base powyżej 162 punktów w konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 2 procesory
Pamięć operacyjna	512 GB RDIMM DDR4 2933 MT/s w modułach o pojemności minimum 32GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC, Online Spare oraz Memory Mirror.
Sloty rozszerzeń	3 aktywne gniazda PCI-Express generacji 3, w tym min. 2 gniazda szybkości x16 (szybkość slotu – bus width). Każde z gniazd PCI-Express musi obsługiwać karty sieciowe 10Gb SFP+, czyli musi istnieć możliwość zainstalowania do każdego slotu karty sieciowej 10Gb SFP+.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy oraz możliwość zainstalowania 1 dysku SFF SAS/SATA/SSD, 2,5” z tyłu serwera. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Serwer wyposażony w 2 dyski 480GB SSD SATA Mixed Use w RAID1.

Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
Interfejsy sieciowe	Serwer musi być wyposażony w: • 1 dwuportowa karta 10Gb Ethernet SFP+, do karty należy dołączyć 2 sztuki wkładek 10Gb SFP+ SR; • 2 jednoportowe karty 16Gb FC z wkładkami komunikacyjnymi 16Gb SFP+ SW; • 4 porty 1GbE RJ45.
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy o: • dodatkowy port DisplayPort dostępny z przodu serwera bez stosowania jakichkolwiek przejściówek; • port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się też stosowania przejściówek na kartach PCI.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 500W.
Napęd	Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW
Karta/moduł zarządzający	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej wymaganej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • dostęp do karty zarządzającej poprzez: - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera; • dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI); - z poziomu linii komend; • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów; • monitorowanie zasilania oraz zużycia energii przez serwer z możliwością graficznej prezentacji; • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping);

	• zdalna aktualizacja oprogramowania (firmware); • wsparcie dla Microsoft Active Directory.
System monitorowania i analizowania konfiguracji serwerów	Dostęp do systemu wymagany jest dla każdego oferowanego serwera. Jeżeli wymaga to dodatkowych licencji, to należy takie licencje dostarczyć. System musi być w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT Zamawiającego. Platforma wspierana uczeniem maszynowym i analizą predykcyjną, zapewniająca automatyczne zbieranie i analizę danych z modułów zarządzania serwerami w celu monitorowania, analizy ich pracy i porównania zachowania serwerów z danymi z referencyjnej bazy danych wszystkich podłączonych do tego systemu serwerów. System musi zapewniać: • scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); • informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; • prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; • rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom; • analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania; • prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach; • zalecenia dotyczące eliminacji źródeł/przyczyn problemów wydajnościowych serwerów.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019 lub nowszy Red Hat Enterprise Linux (RHEL) 7.x lub nowszy SUSE Linux Enterprise Server (SLES) 12 lub nowszy VMware ESXi 6.7 lub nowszy
Wsparcie techniczne	3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji w miejscu instalacji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. Uszkodzone dyski pozostają własnością Zamawiającego.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

IV. Serwer kopii zapasowych danych – 1 szt.

Realizacja zadania uwzględnia m.in.:

1. Dostarczenie, montaż i instalacja kompletnego urządzenia w szafie RACK Zamawiającego.
2. Podłączenie dostarczonego serwera kopii zapasowych do infrastruktury sieciowej LAN oraz SAN Zamawiającego z zachowaniem redundancji połączeń, z zachowaniem rekomendacji producenta.
3. Rekonfigurację sieci SAN i LAN, zapewniającą dostęp do zasobów sieciowych Zamawiającego.
4. Konfigurację oprogramowania systemowego i jego aktualizacja do najnowszej wersji, rekomendowanej przez producenta.
5. Dostarczenie kompletnego okablowania i licencji niezbędnych do uruchomienia urządzenia, zintegrowania ze środowiskiem informatycznym Zamawiającego, z zapewnieniem spełnienia wymaganych funkcjonalności.
6. Wszelkie czynności konfiguracyjne zapewniające prawidłowy dostęp do obecnych zasobów, które muszą zostać wykonane dodatkowo w środowisku Zamawiającego. Zamawiający wymaga, aby wszelkie czynności konfiguracyjne, które są działaniami pośrednimi w celu osiągnięcia wymaganej funkcjonalności, były wykonane w sposób zalecany przez producenta posiadanych oraz dostarczanych urządzeń i oprogramowania.
7. Wykonawca dostarczy kompletne okablowanie i/lub moduły i licencje niezbędne do uruchomienia serwerów i zintegrowania ich ze środowiskiem informatycznym Zamawiającego.

Specyfikacja serwera kopii zapasowych:

Element / cecha	Charakterystyka (wymagania minimalne)
Obudowa	Maksymalnie 2U RACK 19 cali wraz z szynami montażowymi i ramieniem na kable.
Procesor	Jeden procesor 10-rdzeniowy, x86 - 64 bity, Intel Xeon 4210 (2.2GHz/10-core/85W) lub równoważne procesory dziesięciordzeniowe, osiągające w testach SPECrate2017_int_base powyżej 110 punktów w konfiguracji dwuprocesorowej. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 2 procesory
Pamięć operacyjna	32 GB RDIMM DDR4 2933 MT/s w modułach o pojemności minimum 16GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację minimum 3TB pamięci RAM. Obsługa zabezpieczeń: Advanced ECC, Memory Mirror, Online Spare (Rank Sparing).

Sloty rozszerzeń	Serwer musi być wyposażony w: • 3 aktywne gniazda PCI-Express generacji 3 gotowe do obsadzenia kartami sieciowymi , • każde gniazdo x16 lub x8 (szybkość slotu – bus width) • co najmniej 2 gniazda pełnej wysokości (full height) i pełnej długości (full length). Serwer musi mieć dodatkowo dedykowane dwa sloty PCI-Express: • na kontroler dyskowy; • na kartę sieciową 10Gb Ethernet dwuportową.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.
Zasoby dyskowe	Zatoki dyskowe gotowe do zainstalowania 12 dysków typu Hot Swap, Panel przedni z logo producenta. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Serwer wyposażony w 2 dyski 960GB SSD SATA Mixed Use w RAID 1. Serwer wyposażony w 10 dysków 4TB SAS NL w RAID 6.
Interfejsy sieciowe	Serwer musi być wyposażony w: • 1 dwuportowa karta 10Gb Ethernet SFP+, do karty należy dołączyć 2 sztuki wkładek 10Gb SFP+ SR; • 1 dwuportowa karta 16Gb FC z wkładkami komunikacyjnymi 16Gb SFP+ SW; • 4 porty 1GbE RJ45.
Karta graficzna	Zintegrowana karta graficzna
Porty	4 x USB 3.0 (w tym minimum 2x port wewnętrzny) 1x VGA Możliwość rozbudowy o: • port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Karta/moduł zarządzający i system zarządzania	Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej wymaganej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera;

	• dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI); - z poziomu linii komend; • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów; • monitorowanie zasilania oraz zużycia energii przez serwer z możliwością graficznej prezentacji; • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping); • zdalna aktualizacja oprogramowania (firmware); • wsparcie dla Microsoft Active Directory.
System monitorowania i analizowania konfiguracji serwerów	Dostęp do systemu wymagany jest dla każdego oferowanego serwera. Jeżeli wymaga to dodatkowych licencji, to należy takie licencje dostarczyć. System musi być w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT Zamawiającego. Platforma wspierana uczeniem maszynowym i analizą predykcyjną, zapewniająca automatyczne zbieranie i analizę danych z modułów zarządzania serwerami w celu monitorowania, analizy ich pracy i porównania zachowania serwerów z danymi z referencyjnej bazy danych wszystkich podłączonych do tego systemu serwerów. System musi zapewniać: • scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); • informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; • prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; • rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom; • analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania; • prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach; • zalecenia dotyczące eliminacji źródeł/przyczyn problemów wydajnościowych serwerów.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2019 lub nowszy Red Hat Enterprise Linux (RHEL) 7.x lub nowszy SUSE Linux Enterprise Server (SLES) 12 lub nowszy VMware ESXi 6.7 lub nowszy
Wsparcie techniczne	3-letnia gwarancja producenta w miejscu instalacji.

	Czas reakcji w miejscu instalacji to kolejny dzień roboczy. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. Uszkodzone dyski pozostają własnością Zamawiającego.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
System operacyjny	MS WS19 (16-Core) Standard

V. Biblioteka taśmowa – 1 szt.

Realizacja zadania uwzględnia m.in.:

1. Dostarczenie, montaż i instalacja kompletnego urządzenia w szafie RACK Zamawiającego.
2. Podłączenie dostarczonej biblioteki taśmowej do infrastruktury sieciowej LAN oraz SAN Zamawiającego z zachowaniem redundancji połączeń, z zachowaniem rekomendacji producenta.
3. Rekonfigurację sieci SAN i LAN, zapewniającą dostęp do zasobów sieciowych Zamawiającego.
4. Konfigurację oprogramowania systemowego i jego aktualizacja do najnowszej wersji, rekomendowanej przez producenta.
5. Dostarczenie kompletnego okablowania i licencji niezbędnych do uruchomienia urządzenia, zintegrowania ze środowiskiem informatycznym Zamawiającego, z zapewnieniem spełnienia wymaganych funkcjonalności.
6. Wszelkie czynności konfiguracyjne zapewniające prawidłowy dostęp do obecnych zasobów, które muszą zostać wykonane dodatkowo w środowisku Zamawiającego. Zamawiający wymaga, aby wszelkie czynności konfiguracyjne, które są działaniami pośrednimi w celu osiągnięcia wymaganej funkcjonalności, były wykonane w sposób zalecany przez producenta posiadanych oraz dostarczanych urządzeń i oprogramowania.
7. Wykonawca dostarczy kompletne okablowanie i/lub moduły i licencje niezbędne do uruchomienia biblioteki taśmowej i zintegrowania jej ze środowiskiem informatycznym Zamawiającego

Specyfikacja biblioteki taśmowej:

Element / cecha	Charakterystyka (wymagania minimalne)
Obudowa	Wysokość oferowanej biblioteki taśmowej nie może przekraczać 3U. Biblioteka musi być przystosowana do montażu w szafie 19”. Oferowana biblioteka musi być wyposażona w co najmniej 40 slotów na taśmy magnetyczne.

Napędy	Biblioteka taśmowa musi być wyposażona w dwa napędy LTO Ultrium-7 FC. Oferowany napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie co najmniej 101-300MB/s.
Czytnik kodów	Biblioteka taśmowa musi być wyposażona w czytnik kodów kreskowych.
Mail slot	Biblioteka musi posiadać możliwość konfiguracji co najmniej jeden tzw. „mail slot" umożliwiających wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami.
Parametry	Parametr MTBF musi wynosić co najmniej 125 000 godzin. Parametr MSBF musi wynosić co najmniej 1 000 000 pełnych cykli „załaduj/wyładuj".
Rozbudowa	Biblioteka musi posiadać możliwość rozbudowy biblioteki do minimum 275 wnęk na taśmy magnetyczne, do minimum 20 napędów na taśmy LTO7 lub LTO8.
Zasilacze	Redundantne zasilacze w zestawie (minimum dwie sztuki).
Zarządzanie	Biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.
Gwarancja	Wsparcie serwisowe w ciągu 3 lat z czasem reakcji NBD – Następny dzień roboczy. Nośniki w przypadku awarii zostają u Zamawiającego.
Dodatkowe wymagania	Wraz z biblioteką należy dostarczyć 45 szt. taśm LTO-7 RW wraz z etykietami oraz 1 szt. taśmy czyszczącej. Wraz z biblioteka maja być dostarczone odpowiednie kable FC do serwera, długość min. 5 metrów.

VI. Oprogramowanie do wykonywania kopii zapasowych danych.

Specyfikacja oprogramowania do wykonywania kopii zapasowych:

Element / cecha	Charakterystyka (wymagania minimalne)
Wymagania funkcjonalne oprogramowania	1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), pozwalającej na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych. 2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia. 3. Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizycznym (minimum 2xCPU po 8 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V. 4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15

	minut. Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego. 5. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji. 6. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich. 7. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów. 8. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania. 9. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie. 10. System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu. 11. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej. 12. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ. 13. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtedy automatycznie zestawia połączenie tunelowe. 14. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interfejsu musi odbywać się co najmniej poprzez nazwę domeny, sieć, zakres IP. 15. Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania. 16. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN.

	17. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 100 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowych dysków czy macierzy dyskowej). 18. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh. 19. Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie dedupplikacyjnej. 20. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych. 21. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB. 22. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji. 23. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu. 24. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej. 25. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych. 26. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces

	odtwarzania (nawadniania) zdeduplikowanych danych nie wykorzystuje bazę deduplikacyjną. 27. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu. 28. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on" – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną. 29. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD. 30. System musi pozwalać na zarządzanie z poprzez „cmd" z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH. 31. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach. 32. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych). 33. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail. 34. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu. 35. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem.

	36. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO. 37. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password. 38. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrujących – minimum dla: • Safenet • Amazon Web Services (AWS) key management service • Microsoft Azure Key Vault. 39. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy. 40. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to: • Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane, • Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot, • Monitorowanie dużych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji. 41. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email. 42. System musi automatycznie wysyłać informacje o alertach, zdarzeniach oraz informacjach audytowych do syslog serwera. 43. Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach. 44. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to: • Raport zmian/wzrostu środowiska systemu • Raport wykorzystania licencji • Raport wykonanych zadań backupowych 45. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail. 46. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV. 47. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryteriów: • Czas zadania dłuższy niż zadany

	• Ilość danych większa niż …. • Ilość danych mniejsza niż …. • Ilość nie zbackupowanych plików większa niż • Ilośc nie zbackupowanych plików większa niż …% • Wielkośc backupowanych danych wieksza niż … 48. Notyfikacje alertów muszą być wysyłane minimum poprzez mail. 49. Raport spełnienia wymogów SLA dla parametrów: • Ilości dodatkowych kopii backupowych • RTO • RPO 50. System musi zapewniać funkcjonalność wznawiania zadań backupowych. 51. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych. 52. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy. 53. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu. 54. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków. 55. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego. 56. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych. 57. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji. 58. System ma realizować procesy backupu oraz odzyskiwania danych. 59. System ma umożliwić tworzenie zadań backupowych w oparciu o kalendarz.

	60. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane backupowane i archiwizowane. 61. System musi realizować funkcjonalność weryfikacji wykonanych kopii. 62. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów: • Windows: 2016/2012/2008/2003/10/8.1/8/7/Vista • Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu • Unix: AIX/Solaris • OpenVMS 63. System musi umożliwiać (jako opcja) integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri, Kaminario, z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji. 64. System musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe i taśmowe. 65. System powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon. 66. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows. 67. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików. 68. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL). 69. System (jako opcja) powinien umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryteriów powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log. 70. Możliwość odtwarzania backupów plikowych poprzez udostepnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS. 71. System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux. 72. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix. 73. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Red Flag Linux, Scientific Linux, Ubuntu, Slackware.

	74. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris. 75. System musi wspierać funkcjonalność odtwarzania fizycznego serwera do środowiska wirtualnego, minimum: dla serwera Windows do środowiska Vmware. 76. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane. 77. System musi wspierać czołowe rozwiązania wirtualizacyjne: VMware, Hyper-V, Citrix Xen, RHEV, OracleVM, Docker, OpenStack, oVirt, Huawei FusionCompute, Nutanix Acropolis, OpenShift. To znaczy musi posiadać dedykowanego agenta do backupu minimum całej maszyny wirtualnej bez konieczności instalowania agenta wewnątrz maszyny. 78. System musi wspierać wersje środowisk VMware 4.1, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7 poprzez integrację z vStorage API. 79. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS. 80. System musi wspierać środowisko Xen: Citrix XenServer 6.0, 6.1, 6.2, 6.5 81. System musi wspierać środowisko Hyper-V dla: • Microsoft Windows Server 2008 R2 SP1 • Microsoft Windows Server 2012 • Microsoft Hyper-V Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Hyper-V Server 2012 R2 • Microsoft Windows Server 2016 (z Core Edition) • Microsoft Hyper-V Server 2016 (z Core Edition) • Microsoft Windows Server, version 1709 (z Core Edition) • Microsoft Hyper-V Server, version 1709 (z Core Edition) 82. System w kontekście platform VMware i Hyper-V - w przypadku kopii pliku maszyny wirtualnej musi wspierać granularne odtwarzanie pojedynczych plików. 83. System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych. 84. System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej – minimum dla Vmware.

	85. System musi umożliwiać odtworzenie zbackup'owanej maszyny wirtualnej VMware na środowisko Hyper-V. 86. System musi umożliwiać rozbudowę o moduł do zarządzania cyklem życia maszyn wirtualnych (włącznie z możliwością archiwizacji maszyn) co najmniej dla VMware. 87. System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V. 88. System musi umożliwiać (jako opcja) konwersję maszyny wirtualnej do chmury minimalne wsparcia to: Vmware to Azure, Vmware to AWS. 89. Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure. 90. System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik. 91. System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny. 92. Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów. 93. Konfiguracja agentów backupowych dla: MS SQL, Oracle, MySQL musi odbywać się poprzez interfejs graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie. 94. System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników. 95. System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange. 96. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, Postgres, MySQL, Informix, MS SQL.

	97. Dla minimum MySQL i Postgres musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego. 98. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, Notes, SAP/Oracle. 99. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio. 100. Wsparcie dla backupu online dla minimum MS SQL Server 2016/2014/2012/2008/2005. 101. Dedykowany agent bazodanowy dla backupu MS SQL na platformie Linux: Ubuntu, SuSe, RHEL. 102. Możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML. 103. Dedykowani agenci (jako opcja) do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk. 104. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, MySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów. 105. Możliwość backupu i odtwarzania (jako opcja) dokumentów dla Office 365. 106. System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach: • System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh. • Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android. • Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa. • System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i destopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny.

	• System musi oferować możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły). • Każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to: - Odtwarzanie własnych danych - Uruchomienie backupu - Wstrzymanie backupu - Możliwość zdefiniowania innego okna backupowego - Możliwość monitorowania postępu działania zadania - Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN) • Zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane. • Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub). 107. Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych. 108. System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak: • Oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych. • Oprogramowanie musi obsługiwać strategię wielowarstwowego aktywnego archiwum. Na przykład, umożliwiać przenoszenie zarchiwizowanych plików pomiędzy różnorodnymi urządzeniami

	pamięci masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu przejrzystego jedno- krokowego odzyskiwania dla użytkowników końcowych. • Oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych. • Oprogramowanie musi wspierać proces archiwizacji bezpośrednio na taśmy. • Oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej. • Oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów. 109. Oprogramowanie musi umożliwiać (jako opcja) raportowanie wszystkich zadań archiwizacyjnych i odtworzeniowych dla celów zgodności z przepisami/normami bezpieczeństwa (compliance). 110. System musi umożliwiać (jako opcja) pełnokontekstowe indeksowania treści danych dla wybranych typów plików, indeksacja musi odbywać się dla danych znajdujących się już w systemie. 111. System musi umożliwiać (jako opcja) przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji. 112. System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie. 113. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym. 114. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell. 115. Wsparcie dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O).

	116. System musi zamierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum: a. Identyfikacja taśm, które muszą być wyciągnięte z biblioteki b. Identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej c. Automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów d. Identyfikacja i monitorowanie nośników (taśm) w trakcie transportu 117. Możliwość backupu skrzynek pocztowych Google i Google drive. 118. Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy.
Licencjonowanie	1. Sposób licencjonowania dla systemu musi opierać się na ilości serwerów/hostów – dla serwerów fizycznych, a dla środowisk wirtualnych na ilości maszyn wirtualnych lub fizycznych CPU wirtualizatorów podlegających zabezpieczeniu. 2. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu 3. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na nielimitowana ilość bibliotek taśmowych i napędów fizycznych. 4. Oferowana licencja musi pozwalać na nielimitowana budowę architektury systemu backupowego czy to w jednej czy w wielu lokalizacjach. 5. W przypadku wielu lokalizacji licencja musi pozwalać na replikację danych po deduplikacji pomiędzy lokalizacjami. 6. Zaoferowane licencje na system muszą zapewnić backup środowiska o wielkości: • 40 maszyn wirtualnych • 2 serwery fizyczne
Gwarancja	1. Do dostarczonych licencji jest wymagane 36 miesięczne wparcie producenta lub jego autoryzowanego partnera serwisowego (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. 2. Oferowane wsparcie serwisowe musi być świadczone przez producenta rozwiązania lub autoryzowanego partnera serwisowego producenta na terenie Polski. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest

	potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 na świadczone usługi serwisowe.
Uwagi dodatkowe	1. Pojęcie „system” wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie niezintegrowanych pomiędzy sobą wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji. 2. Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych lub pocztowych do archiwum (repozytorium dyskowe lub taśmowe) z pozostawieniem skrótów lub bez ich pozostawiania. 3. Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność. 4. W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

VII. Rozbudowa macierzy dyskowej.

Realizacja zadnia uwzględnia m.in.:

1. Rozbudowę użytkowanej przez Zamawiającego macierzy dyskowej HPE MSA 2040 SAN Storage o dodatkową półkę dyskową, wraz z dyskami.
2. Dostarczenie, montaż i instalację urządzeń w szafie RACK Zamawiającego w lokalizacji DRC i wykorzystana na potrzeby infrastruktury DRC jako zasób dyskowy drugiego klastra VMware.
3. Rekonfigurację sieci SAN i LAN, zapewniającą dostęp do zasobów sieciowych Zamawiającego.
4. Wykonawca dostarczy kompletne okablowanie i/lub moduły i licencje niezbędne do uruchomienia rozbudowanej macierzy dyskowej i integracji jej ze środowiskiem informatycznym Zamawiającego.
5. Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są

dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

Specyfikacja:

Oznaczenie producenta	Opis	Ilość (szt.)
Q1J07B	HPE MSA 2050 SFF Disk Enclosure	1
J9F48A	HPE MSA 1.2TB 12G SAS 10K 2.5in ENT HDD	12
J9F48A#0D1	Factory integrated	12
H7J33A3	HPE 3Y Foundation Care NBD wDMR Service	1
H7J33A3#RC2	HPE MSA 2050 Disk Enclosure Support	1

VIII. Rozbudowa serwerów.

Realizacja zadnia uwzględnia m.in. rozbudowę użytkowanych przez Zamawiającego dwóch serwerów HP DL380 Gen10, przeznaczonych do wykorzystania na potrzeby infrastruktury w ośrodku DRC (jako serwery drugiego klastra VMware).

Specyfikacja:

Oznaczenie producenta	Opis	Ilość (szt.)
455883-B21	HPE BLc 10G SFP+ SR Transceiver	4
815100-B21	HPE 32GB 2Rx4 PC4-2666V-R Smart Kit	16
P9D94A	HPE SN1100Q 16Gb 2p FC HBA	2

IX. Rozbudowa licencji na oprogramowanie Microsoft.

Realizacja zadnia uwzględnia m.in. dostawę dodatkowych licencji Windows Server 2019 Datacenter. Potwierdzenie dot. określonej licencji musi się znaleźć na koncie Zamawiającego, w portalu *Centrum obsługi licencjonowania zbiorowego (Volume Licensing Service Service Center - VLSC) firmy Microsoft*, na podstawie elektronicznego dokumentu dostarczonego przez Wykonawcę.

Specyfikacja:

Oznaczenie producenta	Opis	Ilość (szt.)
9EA-01063	WinSvrDCCore 2019 OLP 2Lic NL Gov CoreLic Qlfd	4

X. Rozbudowa licencji na oprogramowanie VMware.

Realizacja zadnia uwzględnia m.in. rozbudowę (upgrade) posiadanych przez Zamawiającego licencji firmy VMware:

VMware vCenter Server Essentials for vSphere (1 szt.)
VMware vSphere Essentials for 1 processor (6 szt.)
Contract ID: 485013695 (aktywny do: 10.04.2022r.)
Support Level: Subscription Only
ACCOUNT: 114028422 - Urzad Miejski w Nysie

Potwierdzenie dot. określonej licencji musi się znaleźć na koncie Zamawiającego, w portalu firmy VMware. Zamawiający dopuszcza by wsparcie świadczone było przez producenta serwerów posiadanych przez Zamawiającego (Hewlett Packard Enterprise) z możliwością późniejszej migracji do firmy VMware.

Specyfikacja:

Opis	Ilość (komplet)
VMware vSphere 7 Essentials to vSphere 7 Essentials Plus Kit for 3 hosts (Max. 2 processors per host) z 3 letnim wsparciem technicznym.	1

XI. Szkolenia – oprogramowanie wykonywania kopii zapasowych.

W ramach realizacji zadania Wykonawca przeprowadzi szkolenie – instruktaż stanowiskowy dla trzech pracowników wskazanych przez Zamawiającego w zakresie wdrożonego oprogramowania wykonywania kopii zapasowych, niezbędnym do samodzielnego zarządzania i administrowania wdrożonym systemem.

Szkolenia powinny być przeprowadzone w formie min. 4-dniowych warsztatów praktycznych:

a) przez inżyniera posiadającego wiedzę i doświadczenie w obszarze wdrożonego systemu kopii bezpieczeństwa,

b) w dowolnie wybranym terminie, dla którego przekazany zostanie pełen zakres tematyczny szkolenia,

c) nie później niż w ciągu 12-ciu miesięcy od podpisania protokołu odbioru końcowego,

d) na terytorium RP,

e) na sprzęcie udostępnionym przez organizatora szkoleń lub Wykonawcę,

f) w języku polskim,

g) w warunkach zgodnych z przepisami bezpieczeństwa i higieny pracy.

Wszelkie koszty związane z przeprowadzeniem szkolenia, w tym wyżywienie uczestników szkolenia, pokrywa Wykonawca lub organizator szkolenia.

Minimalny zakres instruktarzu obejmuje:

a) opis architektury wdrożonego rozwiązania,

b) sposób i mechanizmy backupu i odtwarzania danych,

c) rodzaje kopii (pełne, przyrostowe), deduplikacja,

d) instalacja, konfiguracja i administrację oprogramowania po stronie serwera i klienta backupu,

e) diagnostykę, monitorowanie pracy i wydajności,

f) obsługę mediów dyskowych i taśmowych,

g) obsługę klientów backupu dla oprogramowania aplikacyjnego i bazodanowego,

h) rozwiązywanie podstawowych problemów w działaniu i funkcjonowaniu systemu backupu,

i) tworzenie i modyfikację grup dyskowych i wolumenów logicznych macierzy,

j) ochronę danych na macierzy,

k) monitorowanie pracy i wydajności macierzy,

l) upgrade firmware'u i oprogramowania macierzy.

Wykonawca, na co najmniej 14 dni przed rozpoczęciem szkolenia, przedstawi Zamawiającemu do akceptacji zakres tematyczny szkolenia.

XII. Szkolenia – oprogramowanie VMware.

W ramach realizacji zadania Wykonawca zapewni szkolenia autoryzowane przez firmę VMware. Szkolenia muszą być realizowane na ternie Polski, w autoryzowanym ośrodku, z zapewnieniem noclegów. Za zgodą Zamawiającego szkolenia mogą być zrealizowane w formie szkoleń on-line. Zamawiający dopuszcza vouchery/bony z możliwością ich realizacji w okresie co najmniej 12 miesięcy od dnia podpisania protokołu odbioru końcowego.

Specyfikacja:

Oznaczenie producenta	Opis	Ilość uczestników
VMW_VSFT7	VMware vSphere: Fast Track [V7]	1
VMW_NSXICM64	VMware NSX: Install Configure Manage [V6.4]	1

XIII. Przedłużenie wsparcia dla licencji Vmware

Realizacja zadania uwzględnia dostawę kontraktu serwisowego, na kolejne 12 miesięcy (liczone od dnia zakończenia aktualnego kontraktu), dla posiadanych przez Zamawiającego licencji na oprogramowania firmy VMware:

VMware vCenter Server Standard for vSphere (1 szt.)
VMware vSphere 6 Enterprise Plus for 1 processor (4 szt.)
Contract ID: 417278983 (aktywny do: 31.12.2020r.)
Support Level: Basic Support
ACCOUNT: 114028422 - Urzad Miejski w Nysie

Specyfikacja:

Lp.	*Opis*	*Ilość licencji*
1.	VS6-EPL-G-SSS-C Basic Support/Subscription VMware vSphere 6 Enterprise Plus for 1 processor for 1 year	4
2.	VCS6-STD-G-SSS-C Basic Support/Subscription VMware vCenter Server 6 Standard for vSphere 6 (Per Instance) for 1 year	1

XIV. Opracowanie dokumentacji.

1. W ramach realizacji zadania Wykonawca w terminie do 10 dni od dnia podpisania umowy opracuje i przedłoży Zamawiającemu do akceptacji projekt techniczny opisujący założenia, etapy oraz proces przeprowadzenia wdrożenia w infrastrukturze informatycznej Zamawiającego wraz z założeniami konfiguracyjnymi. Projekt techniczny zawierać będzie szczegółowy zakres reorganizacji infrastruktury teleinformatycznej Zamawiającego, instalacji i konfiguracji wszystkich urządzeń dostarczanych, rozbudowywanych oraz posiadanych (podlegających rekonfiguracji).
2. Niezwłocznie po zaakceptowaniu przez Zamawiającego przedłożonego projektu technicznego Wykonawca opracuje i przedłoży Zamawiającemu do akceptacji harmonogram prac z uwzględnieniem zaangażowania w pracach Zamawiającego.
3. Wykonawca najpóźniej 2 dni przed upływem terminu wykonania przedmiotu umowy przedstawi do zatwierdzenia dokumentację powykonawczą, obejmującą ponadto:
    a) charakterystykę ogólną dokumentacji, przedmiot opracowania, podstawę opracowania, zakres opracowania, itp.,
    b) opis techniczny zawierający informacje dotyczące zastosowanych urządzeń oprogramowania, parametrów i zastosowanych rozwiązań technologicznych,
    c) specyfikacje urządzeń użytych we wdrożeniu,
    d) schematy połączeń wraz z adresacją IP,
    e) opis czynności konfiguracyjnych wykonanych podczas wdrożenia zobrazowanych zrzutami ekranu, fragmentami skryptów itp.,
    f) opis zmian w konfiguracji i sposobie połączeń działających w środowisku Zamawiającego urządzeń,
    g) procedury instalacyjne i odtworzeniowe na wypadek awarii rozwiązania, w tym serwera backupu,
    h) procedury podłączania nowych hostów do systemu kopii bezpieczeństwa,
    i) procedury wykonywania kopii i odzysku dla wykorzystywanych przez Zamawiającego technologii takich jak m.in. serwery wirtualne VMware i Hyper-V, bazy danych Oracle, Postgres, MySQL, MS SQL, biblioteka taśmowa,
    j) procedury monitorowania pracy urządzeń i oprogramowania,
    k) procedury okresowych czynności administracyjnych dotyczących sprzętu i oprogramowania.
4. Wykonawca zobowiązuje się dostarczyć dokumentację powykonawczą oraz wszystkie dokumenty odbiorowe do siedziby Zamawiającego w formie elektronicznej, z wykorzystaniem jednego lub kilku z następujących formatów zapisu plików:
    a) MS Word (wersje ostateczne dokumentów oraz ich wersje robocze),
    b) PDF (wersje ostateczne dokumentów),
    c) MS Excel (w przypadku dużych zestawień tabelarycznych),
    d) HTML,

e) JPG, GIF, PNG,
f) oraz innych za zgodą Zamawiającego.

XV. Usługi wsparcia technicznego.

W ramach wdrożenia Wykonawca zapewni dodatkową (nie mniejszą niż 20) liczbę godzin wsparcia - asysty technicznej - związanej z serwisowaniem dostarczonej infrastruktury sprzętowej i programowej, które zostaną wykorzystane jako pomoc i konsultacje dla pracowników Zamawiającego obsługujących wdrożone rozwiązanie oraz w razie potrzeby wykonania niezbędnej konfiguracji/rekonfiguracji sprzętu i oprogramowania – koniecznych do prawidłowego jego funkcjonowania bądź optymalizacji działania.

Załącznik nr 2

do umowy nr 2020/INF/……
z dnia ……..

Warunki dokonania odbioru końcowego

1. Dokumentem stwierdzającym dokonanie odbioru przedmiotu umowy jest podpisany przez obie strony protokół odbioru końcowego - bez zastrzeżeń.
2. Odbiór nastąpi po dokonaniu pełnej i ostatecznej weryfikacji kompletności i wymaganej przez Zamawiającego funkcjonalności.
3. W razie stwierdzenia podczas odbioru wad w wykonaniu przedmiotu umowy Zamawiający wyznaczy termin na usunięcie stwierdzonych wad. W takim przypadku za datę odbioru uważa się datę odbioru poprawionego, wolnego od wad przedmiotu umowy.
4. Wymaganymi załącznikami do protokołu odbioru końcowego są:
    1) wszystkie sporządzone w czasie wykonywania umowy protokoły związane z dostawą i instalacją,
    2) certyfikaty serwisowe lub gwarancje na dostarczony sprzęt,
    3) certyfikaty licencyjne na dostarczone oprogramowanie,
    4) pozytywne wyniki testów akceptacyjnych,
    5) dokumentacja powykonawcza,
    6) dokument potwierdzający wykupienie szkoleń.
5. Wynik testu/ów akceptacyjnych uznaje się za pozytywny jedynie w przypadku gdy:
    1) nowe licencje, potwierdzenie nabycia wsparcia na oprogramowanie lub sprzęt będą zarejestrowane i widoczne na portalu Producenta z poziomu konta Zamawiającego,
    2) aktywowane zostały licencje zdalnego zarządzania poszczególnymi serwerami oraz możliwy jest zdalny dostęp do konsoli serwera,
    3) dostarczony sprzęt i oprogramowanie zostaną wdrożone w infrastrukturze Zamawiającego zgodnie Projektem Technicznym przedstawionym na etapie wdrożenia przez Wykonawcę i zaakceptowanym przez Zamawiającego,
    4) pomyślnie wykonano backup i odzyskano maszyny wirtualne Windows i Linux działającą w klastrze Vmware. W przypadku Vmware zweryfikowano, iż backup jest możliwy poprzez sieć LAN jak i SAN,
    5) pomyślnie wykonano backup i odzyskano maszyny wirtualne Windows i Linux na działających niezależnie od klastra serwerach ESXi,
    6) pomyślnie wykonano backup i odzyskano maszynę wirtualną działającą na Hyper-V,
    7) pomyślnie odzyskano pojedyncze pliki z kopii maszyn wirtualnych (Windows i Linux), zarówno dla Vmware, jak i dla Hyper-V,
    8) pomyślnie wykonano backup Active Directory i odzyskano pojedyncze obiekty (np. konto użytkownika),

9) pomyślnie wykonano backup bazy danych Microsoft SQL Server i odzyskano kopię do działającej instancji MS SQL Server,
10) pomyślnie wykonano backup i odzyskano bazę danych MySQL/MariaDB,
11) pomyślnie wykonano backup i odzyskano bazę danych PostgreSQL,
12) pomyślnie wykonano backup bazy danych Oracle,
13) pomyślnie wykonano przełączenie aktywnych ośrodków PDC – DRC.

Zamawiający: **Wykonawca:**

....

Umowa powierzenia przetwarzania danych osobowych stanowiąca uzupełnienie Umowy 2020/INF/…… z dnia …….r. („Umowa Podstawowa")

zawarta w dniu …….r. w Nysie, pomiędzy:

Gminą Nysa, 48-300 Nysa, ul. Kolejowa 15, NIP 753-24-14-579 zwaną dalej **Administratorem,** reprezentowaną przez:

- Kordiana Kolbiarza – Burmistrza Nysy,

a

……, zwaną/ym dalej **Przetwarzającym,** reprezentowaną/ym przez:

- ……

(dalej łącznie jako: **Strony**).

Mając na uwadze, że:

1) Strony zawarły Umowę Podstawową, w związku z wykonywaniem której konieczne jest powierzenie przez Administratora Przetwarzającemu przetwarzania danych osobowych w zakresie określonym Umową;

2) Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych powierzonych przez Administratora;

3) Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej **RODO** oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

Strony postanowiły zawrzeć Umowę o następującej treści:

§ 1 Opis Przetwarzania

1. Na warunkach określonych niniejszą Umową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.
2. Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.
3. Charakter i cel przetwarzania wynikają z Umowy Podstawowej.
4. Przetwarzanie obejmować będzie dane osobowe („**Dane**"), przetwarzane przy użyciu systemu informatycznego Administratora.
5. Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:
   1) osoby fizyczne
6. Przetwarzanie Danych będzie dotyczyć następujących ich rodzajów:

1) zwykłe,
2) szczególne.

§ 2 Podpowierzenie

1. Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („**Podpowierzenie**") w drodze pisemnej umowy podpowierzenia („**Umowa Podpowierzenia**") innym podmiotom przetwarzającym („**Podprzetwarzający**"), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2. Powierzenie przetwarzania Danych Podprzetwarzającym wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu w terminie 14 dni od dnia otrzymania zgłoszenia. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

3. Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

4. Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

5. Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

§ 3 Obowiązki Przetwarzającego

1. Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami oraz instrukcjami Administratora, których potwierdzeniem jest zawarcie niniejszej Umowy.

2. Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („**EOG**")). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

3. Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych przy wykonaniu przedmiotu niniejszej Umowy, udokumentowane zobowiązania do

zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

4. Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

5. Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego), określonych w § 2.

6. Przetwarzający zobowiązuje się współpracować i wspierać Administratora, poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („**Prawa jednostki**").

7. Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32−36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

8. Jeżeli Przetwarzający poweźmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

9. W ramach realizacji przez Przetwarzającego zmian w systemie, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych kluczowych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.

10. Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.

11. Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu Administratora zgodnie z art. 30 RODO. Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności kategorii przetwarzania danych Przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

12. Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

13. Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

§ 4 Obowiązki Administratora

Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

§ 5 Bezpieczeństwo danych

1. Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych i stosuje się do jej wyników, co do organizacyjnych i technicznych środków ochrony danych. Na żądanie, Przetwarzający udostępni Administratorowi dokumenty z przeprowadzonej analizy ryzyka.

2. Na żądanie, Przetwarzający przedstawi Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie strony zachowują kopię przedstawionych dokumentów i dowody przedstawienia informacji, dla potrzeb spełnienia wymogu rozliczalności.

§ 6 Powiadomienie o Naruszeniach Danych Osobowych

1. Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.

2. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organu nadzoru.

§ 7 Nadzór

1. Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych. Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.

2. Przetwarzający współpracuje z organem nadzorczym w zakresie wykonywanych przez niego zadań.

3. Przetwarzający:

    1) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

2) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

4. Przetwarzający jest obowiązany powiadomić Administratora o każdej kontroli organu nadzorczego, jeżeli ma ona związek z przetwarzaniem powierzonych danych osobowych oraz o każdym piśmie organu nadzorczego dotyczącym składania wyjaśnień w zakresie powierzonych danych osobowych objętych Umową, chyba, że zawiadomienie takie będzie niedozwolone.

5. Przetwarzający oświadcza, że w przypadku kontroli organu nadzorczego prowadzonej u Przetwarzającego, dotyczącej przetwarzania powierzonych danych osobowych, będzie przekazywał Administratorowi wszelkie informacje i wyjaśnienia.

6. Jeżeli w wyniku zawinionego niewłaściwego przetwarzania danych osobowych przez Przetwarzającego, Administrator zostanie prawomocnym orzeczeniem zobowiązany do wypłaty odszkodowania, zadośćuczynienia lub zostanie ukarany grzywną, Przetwarzający zobowiązuje się zrekompensować Administratorowi udokumentowane straty z tego tytułu do wysokości poniesionego prawomocnie zasądzonego odszkodowania, zadośćuczynienia lub grzywny. Zobowiązanie Przetwarzającego o którym mowa powyżej, powstanie pod warunkiem pisemnego powiadomienia go o każdym przypadku wystąpienia roszczeń wobec Administratora i jego podstawach prawnych i faktycznych, w terminie nie później niż 14 dni od dnia otrzymania takiego roszczenia, w celu umożliwienia Przetwarzającemu zajęcia stanowiska, odniesienia się do podstaw takiej odpowiedzialności i ewentualnego wstąpienia do sprawy na etapie sądowym.

7. Przetwarzający jest zwolniony z odpowiedzialności za szkody spowodowane przetwarzaniem naruszającym przepisy prawa jeśli nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

§ 8 Oświadczenia Stron

1. Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

2. Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umową posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

3. Na żądanie Administratora Przetwarzający okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe lub inne dowody, iż Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

§ 9 Odpowiedzialność

1. Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

2. Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, odpowiedzialność solidarną wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

§ 10 Usunięcie Danych

1. Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:

    a) usunięcia Danych,

    b) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.

2. Przetwarzający dokona usunięcia Danych w terminie nie dłuższym niż 5 dni od zakończenia Umowy, chyba że Administrator poleci mu to uczynić wcześniej.

3. Po wykonaniu zobowiązania, o którym mowa w ust.1., Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

§ 11 Postanowienia Końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

2. Umowa podlega prawu polskiemu oraz RODO.

3. Z tytułu zawarcia umowy, Administrator nie ponosi żadnych dodatkowych kosztów, a Przetwarzającemu nie przysługuje żadne dodatkowe roszczenie względem Administratora.

Administrator **Przetwarzający**