OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Dostawa i montaż deduplikatorów wraz ze wsparciem technicznym, gwarancją na okres 60 miesięcy oraz wdrożeniem rozwiązania.

II. Oznaczenie przedmiotu zamówienia wg CPV

30233000-1 – urządzenia do przechowywania i odczytu danych
71356300-1 – usługi wsparcia technicznego

III. Definicje

W Opisie Przedmiotu Zamówienia, dalej: „OPZ", poniższym pojęciom nadaje się następujące znaczenie:

Lp.	Termin	Definicja
1.	**Awaria**	Nieprawidłowe działanie Urządzeń lub Oprogramowania, w szczególności brak możliwości używania Urządzeń lub Oprogramowania w sposób zgodny z ich przeznaczeniem lub z dokumentacją producenta lub dokumentacją powykonawczą.
2.	**Awaria Krytyczna**	Awaria skutkująca brakiem działania systemu lub spowolnieniem działania uniemożliwiającym korzystanie z kluczowych jego funkcji.
2.	**Dni Robocze**	Dni od poniedziałku do piątku oprócz dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej;
3.	**Dokumentacja**	Wszelkie dokumenty i instrukcje dołączane przez producenta Urządzeń lub Oprogramowania, jeśli występują.
4.	**Dokumentacja powykonawcza**	Dokumentacja wykonanej instalacji przedmiotu zamówienia, zawierająca opis wykonanych prac, schemat rozmieszczenia Urządzeń, konfigurację Oprogramowania, graficzne schematy połączeń, itp.
5.	**Etap**	Określona część zamówienia
6.	**Godziny eksperckie**	Usługi konsultacji, opisane w punkcie Świadczenie usług Godzin eksperckich OPZ
7.	**Lokalizacja**	Dwa miejsca na terenie miasta stołecznego Warszawy, do których ma nastąpić dostawa przedmiotu zamówienia. Dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po podpisaniu Umowy.

8.	**Opcja (prawo opcji)**	Uprawnienie Zamawiającego do rozszerzenia zakresu zamówienia o prace w ramach Godzin eksperckich, szczegółowo opisane w punkcie Świadczenie usług Godzin eksperckich w ramach prawa opcji OPZ. Przedmiotowe uprawnieni będzie realizowane każdorazowo na Zlecenie Zamawiającego.
9.	**Oprogramowanie**	Całość lub dowolny element oprogramowania dostarczanego w ramach realizacji zamówienia zgodnie z opisem w OPZ.
10.	**Protokół Odbioru Ilościowego**	Protokół potwierdzający prawidłowe wykonanie dostawy przedmiotu zamówienia w zakresie wskazanym w OPZ.
11.	**Protokół Odbioru Jakościowego**	Protokół potwierdzający prawidłowe wykonanie Montażu lub Wdrożenia przedmiotu zamówienia w zakresie wskazanym w OPZ.
12.	**Serwis gwarancyjny**	Naprawa Urządzeń stanowiących przedmiot zamówienia zgodnie z warunkami opisanymi w punkcie Warunki świadczenia usług gwarancji/serwisu gwarancyjnego w OPZ.
13.	**Urządzenia**	Wszystkie urządzenia stanowiące przedmiot zamówienia zgodnie z opisem i minimalną konfiguracją opisaną w OPZ.
14.	**Warsztaty**	Przeprowadzony przez Wykonawcę instruktaż w zakresie wdrożonych Urządzeń i Oprogramowania.
15.	**Wdrożenie**	Montaż oraz uruchomienie Urządzeń i Oprogramowania w Lokalizacja Zamawiającego.
16.	**Wsparcie techniczne**	Wsparcia technicznego Oprogramowania stanowiące przedmiot zamówienia zgodnie z warunkami opisanymi w punkcie Warunki świadczenia wsparcia technicznego w OPZ.
17.	**Zgłoszenie awarii**	Poinformowanie Wykonawcy przez Zamawiającego o wystąpieniu Awarii na zasadach opisanych w punkcie Warunki świadczenia usług gwarancji/serwisu gwarancyjnego lub Warunki świadczenia wsparcia technicznego
18.	**Zlecenie**	Dokument zawierający zlecenie wykonania usługi Godzin eksperckich, zgodnie z opisem w OPZ.

IV. Przedmiot Zamówienia

Przedmiotem zamówienia jest:

1) **W ramach zamówienia podstawowego:**
   a) Dostawa deduplikatorów, o których mowa w pkt X tabela nr 1 OPZ – 2 sztuki,
   b) Dostawa autoryzowanych szkoleń, o których mowa w pkt X tabela nr 2 OPZ – dla 5 osób,
   c) Wykonanie Projektu Technicznego, o którym mowa w pkt X tabela nr 3 OPZ,
   d) Przeprowadzenie wdrożenia dostarczonych Urządzeń wraz z Dokumentacją powykonawczą, o którym mowa w pkt X tabela nr 4 OPZ,
   e) Przeprowadzenie Warsztatów, o których mowa w pkt X tabela nr 5 OPZ.

2) **W ramach opcji:**
   a) Zapewnienie usługi Godzin Eksperckich, o którym mowa w pkt VIII OPZ – maksymalnie do 500 godzin

   Zamówienie realizowane w ramach opcji jest jednostronnym uprawnieniem Zamawiającego, dlatego też nieskorzystanie przez Zamawiającego z opcji nie stanowi podstawy dla Wykonawcy do dochodzenia jakichkolwiek roszczeń w stosunku do Zamawiającego.

   Zamawiający zastrzega możliwość skorzystania z opcji w ciągu 12 miesięcy od daty zawarcia Umowy.
3) **Zapewnienie Gwarancji** dla Urządzeń na okres 60 miesięcy, o której mowa w pkt. IX OPZ,
4) **Zapewnienie Wsparcia technicznego** dla Oprogramowania na okres 60 miesięcy wraz z udzieleniem licencji na Oprogramowanie, o którym mowa w pkt. VIII OPZ.

V. Terminy realizacji przedmiotu zamówienia

1. Wykonawca zapewni realizację przedmiotu zamówienia w następujących terminach:
   a. Wykona dostawę Urządzeń, o których mowa w pkt X tabela nr 1 OPZ w ciągu 45 dni od dnia zawarcia umowy, która nastąpi do Lokalizacji, wraz z Oprogramowaniem, Dokumentacją, w Godzinach roboczych oraz zapewnieniem Gwarancji i Wsparcia technicznego;
   b. Wykona Projekt Techniczny w ciągu 30 dni od daty zawarcia umowy,
   c. Przeprowadzi Wdrożenie w ciągu 30 dni od daty dostawy Urządzeń,
   d. Przeprowadzi Warsztaty w ciągu 10 dni od daty zakończenia Wdrożenia,
   e. Dostarczy autoryzowane szkolenia w formie voucherów w ciągu 5 dni od zakończenia Warsztatów.
2. Dostarczone Urządzenia zostaną objęte serwisem gwarancyjnym producenta lub autoryzowanego partnera serwisowego producenta przez okres 60 miesięcy od dnia wskazanego w podpisanym przez strony bez zastrzeżeń Protokole Odbioru Jakościowego Wdrożenia dla poszczególnych Etapów.
3. Dostarczone Oprogramowanie zostanie objęte wsparciem technicznym wraz z dostępem do Aktualizacji, pochodzących z oficjalnego kanału producenta, na okres 60 miesięcy od dnia wskazanego w podpisanym przez strony bez zastrzeżeń Protokole Odbioru Jakościowego Wdrożenia dla poszczególnych Etapów.

VI. Ogólne warunki realizacji przedmiotu zamówienia

1. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa.
2. Urządzenia muszą być fabrycznie nowe, nieużywane wcześniej, muszą być objęte gwarancją producenta oraz posiadać najnowszą dostępną stabilną wersję oprogramowania.
3. Wszelkie opakowania, wypełniacze oraz inne odpady wniesione na teren Lokalizacji w ramach dostawy zostaną zutylizowane przez Wykonawcę chyba że Zamawiający zadecyduje inaczej.
4. Urządzenia muszą być kompletne, tj.: mieć wszystkie komponenty zapewniające właściwą instalację i użytkowanie.
5. Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawa z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2022 r. poz. 1863 z późn. zm.), dalej: „Ustawa", należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym,

Oprogramowanie musi być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

6. W Wraz z Urządzeniami i Oprogramowaniem Wykonawca zobowiązany jest dostarczyć na adres e-mail, który zostanie wskazanym w umowie:

   6.1. Adresy poczty elektronicznej, numery telefonów oraz dane dostępowe do portalu zgłoszeniowego, umożliwiające Zamawiającemu korzystanie z Gwarancji świadczonej przez Wykonawcę;

   6.2. Dokument potwierdzający objęcie Urządzeń Gwarancją producenta wraz z jej szczegółowymi warunkami;

   6.3. Adresy poczty elektronicznej, numery telefonów oraz dane dostępowe do portalu zgłoszeniowego, umożliwiające Zamawiającemu korzystanie z Gwarancji świadczonej przez producenta lub autoryzowanego partnera producenta;

   6.4. Wszystkie wymagane licencje wraz z kluczami licencyjnymi i aktywacyjnymi Oprogramowania (w tym tego dostarczanego wraz z Urządzeniami);

   6.5. Dane, do których są przypisane licencje na danym portalu producenta Oprogramowania;

   6.6. Dokument potwierdzający dostawę licencji na Oprogramowanie (w tym certyfikaty) i objęcie Wsparciem technicznym wraz ze wskazaniem okresu obowiązywania na poziomie zgodnym ze wskazanym w OPZ;

   6.7. Dokumentacja, w szczególności umowa licencyjna, zawierająca warunki licencjonowania danego Oprogramowania określone przez producenta;

   6.8. Adresy poczty elektronicznej, numery telefonów oraz dane dostępowe do portalu klienckiego, umożliwiające Zamawiającemu korzystanie ze Wsparcia Technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie lub autoryzowanego partnera producenta;

   6.9. Aktualne zestawienie w formacie arkusza Excel 2016 (lub nowszego) wszystkich dostarczonych pozycji w zakresie Urządzeń i Oprogramowania zawierające informacje m.in. oznaczenie producenta (tzw. part number), pełna nazwa produktu, metryka licencyjna, wersja i edycja Oprogramowania, rodzaj licencji, okres obowiązywania licencji/Gwarancji/Wsparcia Technicznego, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto, zgodnie z zapisami zawartymi w Ofercie.

VII. Warunki świadczenia usługi godzin eksperckich w ramach opcji

1. W ramach podpisanej umowy Zamawiający jest uprawniony do zlecenia Wykonawcy w ramach opcji świadczenia usługi tzw. Godzin eksperckich certyfikowanego przez Producenta inżyniera w miejscu zainstalowania przedmiotu zamówienia w Dni Robocze, dotyczącej konsultacji, rozwiania wątpliwości lub rozwiązania bieżących problemów Zamawiającego z obsługi przedmiotu zamówienia.

2. W zakresie przedmiotu opcji, rozliczenie wynagrodzenia Wykonawcy będzie następować w oparciu na stawce godzinowej pracy konsultanta, w ramach puli roboczogodzin, z możliwością wykorzystania jej w okresie trwania umowy.

3. Osoby realizujące usługi w ramach Godzin eksperckich muszą legitymować się certyfikatem Producenta lub akredytowanego przez Producenta podmiotu zamówienia, potwierdzającym wiedzę techniczną w zakresie przedmiotu zamówienia na poziomie eksperckim oraz muszą posiadać dostęp do bazy wiedzy tego Producenta.

4. W ramach usług realizowanych jako Godziny eksperckie będą świadczone na **Zlecenie** Zamawiającego m.in.:

   4.1. Wsparcie w obsłudze, konfiguracji oraz eksploatacji wdrożonego środowiska,

4.2. Konsultacje dotyczące modyfikacji (w tym rozbudowy) wdrożonych rozwiązań,
4.3. Asysta przy przełączeniu kopii zapasowych na nowe środowisko,
4.4. Wsparcie pracowników Zamawiającego w zakresie utrzymania środowiska.

VIII. Warunki świadczenia usług Wsparcia Technicznego

1. Wykonawca zobowiązany jest zapewnić Zamawiającemu **Wsparcie Techniczne Oprogramowania** realizowane przez Producenta Oprogramowania, świadczone bezpośrednio lub przez autoryzowany podmiot współpracujący z Producentem w okresie 60 miesięcy, od dnia uruchomienia Urządzeń i podpisania Protokołu Odbioru Jakościowego.
2. W ramach Wsparcia Technicznego dla Oprogramowania, stanowiącego przedmiot zamówienia i opisanego w OPZ Zamawiający ma:
   2.1. prawo do bezpłatnego korzystania z wydawanych przez Producenta najnowszych wersji, Aktualizacji Oprogramowania, poprawek do Oprogramowania;
   2.2. dostęp elektroniczny 24x7x365 do pomocy technicznej;
   2.3. dostęp elektroniczny do bazy wiedzy, dokumentacji, biuletynów i informacji na temat Oprogramowania, posiadanych produktów.
   2.4. Szczegółowe warunki Wsparcia Technicznego dla Oprogramowania regulują umowy licencyjne wydane przez producenta Oprogramowania, z zastrzeżeniem, że nie mogą być mniej korzystane do warunków wskazanych w niniejszym Opisie Przedmiotu Zamówienia.
3. W przypadku Awarii Krytycznej Oprogramowania Wykonawca zobowiązuje się do zapewnienia Czasu reakcji w ciągu 1h od Zgłoszenia. Obsługa Awarii Krytycznych Oprogramowania jest świadczona na zasadach określonych przez producentów tego Oprogramowania.
4. Wszystkie licencje Oprogramowania muszą pozwalać na swobodne przenoszenie pomiędzy Urządzeniami (np. w przypadku wymiany Urządzenia).
5. Wszystkie licencje pochodzić będą z legalnego tj. akceptowanego przez producenta Oprogramowania kanału dystrybucji.
6. Wszystkie licencje pochodzić będą z kanału dystrybucji na teren Unii Europejskiej.

IX. Warunki świadczenia usług Serwisu Gwarancyjnego

W zakresie usługi gwarancyjnej dla Urządzeń Wykonawca zobowiązuje się do zapewnienia poniższego:

1) Urządzenia, mają być fabrycznie nowe, nie używane wcześniej, mają być objęte gwarancją realizowaną przez zespół wsparcia technicznego producenta lub podmiotu autoryzowanego przez producenta oraz posiadać możliwie najnowszą dostępną stabilną wersję Oprogramowania pozwalającą na rozbudowę bez konieczności przerywania pracy posiadanych urządzeń.
2) W przypadku braku możliwości naprawy Urządzeń, w miejsce Urządzenia, które nie może być przez Wykonawcę naprawione, Wykonawca zobowiązany jest do dostarczenia Zamawiającemu innego urządzenia, wolnego od wad, o parametrach technicznych nie gorszych od parametrów technicznych Urządzenia naprawianego oraz zapewniających nie gorszy poziom bezpieczeństwa, objętego gwarancją, przenosząc jego własność na Zamawiającego, oraz dostarczy go do Lokalizacji w ramach wynagrodzenia przewidzianego w umowie, a następnie świadczenia gwarancji w stosunku do tego Urządzenia biegnącej od dnia wskazanego w podpisanym protokole usunięcia Awarii na okres odpowiadający danemu Urządzeniu, o którym mowa w pkt IV ppkt 2) OPZ.
3) **Usunięcie Awarii Krytycznej** Urządzeń, których mowa w pkt IV ppkt 1a, 1b, 1d OPZ poprzez naprawę lub wymianę Urządzeń będzie realizowana przez Wykonawcę w każdy dzień kalendarzowy w ciągu 24 godzin od momentu Zgłoszenia Awarii Krytycznej. Zamawiający dopuszcza zastosowanie obejścia - w przypadku braku możliwości dotrzymania czasu usunięcia Awarii, o którym mowa w zdaniu poprzednim, Wykonawca dostarczy

w tym terminie, na czas usuwania Awarii, w pełni sprawny sprzęt zastępczy, objęty gwarancją, o nie gorszych parametrach niż Sprzęt naprawiany, oraz przygotuje i dostarczy Zamawiającemu dokumenty informujące o wykonanej zamianie w ramach gwarancji, z zastrzeżeniem że wszelkie nośniki z danymi muszą pozostać własnością Zamawiającego. W takim przypadku czas usunięcia Awarii to do 10 Dni Roboczych od dnia Zgłoszenia Awarii przez Zamawiającego. Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu i instalacji.

4) **Usunięcie Awarii** innych niż Awaria Krytyczna Urządzeń, o których mowa w pkt IV ppkt 1a, 1b, 1d OPZ poprzez naprawę lub wymianę Urządzeń będzie realizowana przez Wykonawcę w każdy Dzień Roboczy w ciągu 48 godzin od momentu Zgłoszenia Awarii. Zamawiający dopuszcza zastosowanie obejścia - w przypadku braku możliwości dotrzymania czasu usunięcia Awarii, o którym mowa w zdaniu poprzednim, Wykonawca dostarczy w tym terminie, na czas usuwania Awarii, w pełni sprawny sprzęt zastępczy, objęty gwarancją, o nie gorszych parametrach niż Sprzęt naprawiany, oraz przygotuje i dostarczy Zamawiającemu dokumenty informujące o wykonanej zamianie w ramach gwarancji, z zastrzeżeniem że wszelkie nośniki z danymi muszą pozostać własnością Zamawiającego. W takim przypadku czas usunięcia Awarii to do 15 Dni Roboczych od dnia Zgłoszenia Awarii przez Zamawiającego. Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu i instalacji.
5) W razie niedotrzymania przez Wykonawcę terminu usunięcia Awarii Krytycznej Urządzeń zgodnie z powyższym punktem, Zamawiający ma prawo zlecić jej usunięcie stronie trzeciej, przy czym będzie ona realizowana w całości na koszt Wykonawcy. W takiej sytuacji Zamawiający wezwie Wykonawcę do zaprzestania dalszych działań związanych z obsługą Zgłoszenia oraz przekaże informację o przekierowaniu Zgłoszenia do strony trzeciej.
6) Wszelkie uszkodzone nośniki danych pozostaną własnością Zamawiającego. W przypadku stwierdzenia uszkodzenia nośnika danych nieulotnych (typu dysk twardy, SSD), będzie on wymieniony przez Wykonawcę na nowy, wolny od wad, bez konieczności zwrotu uszkodzonego nośnika danych i dokonywania jego ekspertyzy poza miejscem używania przedmiotu Umowy.
7) Wydanie Sprzętu poza Lokalizację w celu usunięcia Awarii lub zwrot sprzętu zastępczego będą mogły nastąpić dopiero po trwałym usunięciu danych ze wszystkich nośników danych zainstalowanych w Sprzęcie np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez gwaranta w obecności Zamawiającego i zdeponowaniu ich u Zamawiającego.
8) W przypadku, gdy dany Sprzęt ulegnie Awarii po raz trzeci, Wykonawca dokona usunięcia Awarii poprzez wymianę uszkodzonego Sprzętu na nowy, wolny od wad, objęty Gwarancją do dnia upływu okresu Gwarancji wskazanego w pkt IV ppkt 2) OPZ, o parametrach nie gorszych od Sprzętu podlegającego wymianie, przenosząc jego własność na Zamawiającego, oraz dostarczy nowy Sprzęt do Lokalizacji na własny koszt i ryzyko, w terminie 15 Dni Roboczych liczonych od dnia Zgłoszenia trzeciej Awarii.
9) Wszystkie wykonane prace podjęte w celu usunięcia Awarii Urządzeń wymagają potwierdzenia w formie pisemnej lub elektronicznej przez przedstawiciela Zamawiającego. Fakt usunięcia Awarii zostanie potwierdzony protokołem usunięcia Awarii.
10) Usługi gwarancyjne świadczone będą w języku polskim.

X. Szczegółowe wymagania techniczne

1. Deduplikator

Lp.	Nazwa wymagania	Opis wymagania
1.1.	Wymagania ogólne	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
1.2.		Urządzenie musi być rozwiązaniem kompletnym urządzeniem sprzętowym typu appliance pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
1.3.		Wszystkie wymagania wskazane w OPZ muszą być spełnione łącznie – nie może zaistnieć sytuacja, w której spełnienie jednego wymagania powoduje automatyczne niespełnienie innego.
1.4.		Oferowane urządzenie musi być kompatybilne z mechanizmami cyber bunkra opisanymi niżej i umożliwiać jego wdrożenie w trzeciej (oddalonej) Lokalizacji w przyszłości. Dostarczenie funkcjonalności cyber bunkra nie jest elementem tego postępowania.
2.1.	Kontroler	Aktywne kontrolery deduplikatorów muszą posiadać łącznie co najmniej 80 rdzeni w architekturze x86_64 o częstotliwości bazowej 2,1GHz oraz 1 536 GB RAM.
2.2.		Rozwiązanie musi posiadać co najmniej 28TB pamięci cache oparty o pamięć flash.
2.3.		Wymagana konfiguracja wysokodostępna (HA) – min. dwukontrolerowa (n+1), współdzieląca zasoby dyskowe urządzenia. Konfiguracja dwukontrolerowa dotyczy kontrolerów sterujących pracą urządzenia (nie chodzi o ew. kontrolery stosowane w przypadku np.: macierzy dyskowych, które mogą być częścią składową przestrzeni dyskowej deduplikatora), na których zainstalowane jest oprogramowanie zapewniające wymagane funkcjonalności deduplikatora.
2.4.		Konfiguracja wysokodostępna (HA) musi umożliwiać automatyczny fail-over oraz kontynuację pracy urządzenia w przypadku uszkodzenia kontrolera, przy zapewnieniu wymaganych parametrów wydajnościowych oraz utrzymaniu wymaganych funkcjonalności (wymóg konfiguracji HA nie będzie spełniony jeżeli producent oferowanego urządzenia nie oferuje oficjalnie takiej funkcjonalności w obrębie oferowanego typu/modelu urządzenia, oferowana funkcjonalność HA powinna znaleźć potwierdzenie w ogólnie dostępnej dokumentacji dla oferowanego urządzenia).
3.1.	Protokoły dostępu	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: • CIFS, NFS • zapewniającymi deduplikację na źródle (kliencie), wymagane wsparcie dla oferowanego oprogramowania kopii zapasowych • VTL (min. 10 jednocześnie) (po doposażeniu w porty FC)
3.2.		Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia

4.1.	Wydajność i skalowalność	Dostarczone urządzenie musi oferować przestrzeń min. 576TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 2PB netto.
4.2.		Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.
4.3.		Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare.
4.4.		Aktywne kontrolery deduplikatora muszą udostępniać łącznie co najmniej: • 8 portów Eth 25 Gb/s OP • 4 porty FC 32 Gb/s OP Wszystkie porty realizowane są za pomocą redundantnych kart sieciowych w obrębie pojedynczego kontrolera i wyposażone zostaną w odpowiednie wkładki. Wymagana możliwość obsługi każdym z w/w portów protokołów: CIFS, NFS, deduplikacja na źródle.
4.5.		Oferowane urządzenie musi być wyposażone w karty do podłączenia półek dyskowych w ilości umożliwiającej obsługę maksymalnej ich ilości przewidzianej przez producenta deduplikatora.
4.6.		Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: **NFS** co najmniej 70 TB/h (dane podawane przez producenta) oraz co najmniej 130 TB/h z wykorzystaniem **deduplikacji na źródle** (dane podawane przez producenta).
4.7.		Urządzenie musi pozwalać na jednoczesną obsługę minimum 1 800 strumieni w tym jednocześnie: • zapis danych minimum 500 strumieniami, • odczyt danych minimum 300 strumieniami, • replikacja minimum 1 000 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.
4.8.		Wymieniona wartość 1800 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 500 dla zapisu i jednocześnie 300 strumieni dla odczytu i jednocześnie 1000 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
4.9.		Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
5.1.	Funkcjonalność deduplikacji	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.

5.2.		Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A", nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B" w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS).
5.3.		Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
5.4.		Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji. Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
5.5.		Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backupową.
5.6.		Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych interfejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backupowej, dane zapisywane poprzez interfejsy NFS/CIFS bez użycia jakiejkolwiek aplikacji backupowej również muszą być deduplikowane w sposób in-line.
5.7.		Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
5.8.		Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.
5.9.		Oferowane urządzenie musi wspierać oferowane oprogramowanie kopii zapasowych w trybie zapisu deduplikacji na źródle (standardowym kliencie w odróżnieniu od np.: media serwer, storage node czy wirtualny system w oparciu o FUSE). Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych (bloki) nie znajdujące się dotychczas na urządzeniu.
6.1.	Obsługa VTL	Urządzenie musi umożliwiać emulację minimum 400 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów.

6.2.		Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych: • StorageTek L180 • IBM TS3500
6.3.		Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min.: LTO5, LTO7
7.1.	Integracja z systemem kopii zapasowych	Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych, funkcjonalność ta powinna być oficjalnie wspierana przez posiadane przez Zamawiającego oprogramowanie kopii zapasowych. Oficjalnie dopuszczalna przez producenta urządzenia ilość jednocześnie uruchomionych maszyn wirtualnych w takim trybie nie powinna być mniejsza niż 60.
7.2.		Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez posiadane przez Zamawiającego oprogramowanie kopii zapasowych.
7.3.		Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku posiadanego przez Zamawiającego oprogramowania kopii zapasowych.
8.1.	Replikacja	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych. Konfiguracja replikacji musi być możliwa w każdym z trybów: • jeden do jednego • wiele do jednego • jeden do wielu • kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C). Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
8.2.		Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
8.3.		W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
8.4.		W przypadku replikacji danych między dwoma urządzeniami wymagana jest możliwość kontroli funkcjonalności przez oferowane oprogramowanie w następujący sposób: • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących • replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu • replikacja zarządzana jest z poziomu posiadanego przez Zamawiającego oprogramowania kopii zapasowych • oprogramowanie posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
8.5.		Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
9.1.	Kopie migawkowe	Oferowane urządzenie musi umożliwiać wykonywanie snapshotów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze snapshotu.

		Odtworzenie danych z kopii migawkowej nie może wymagać konieczności nadpisania danych produkcyjnych, jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). Wymagana jest możliwość wykorzystania funkcjonalności dla danych przesyłanych dowolnym z wymaganych interfejsów urządzenia.
9.2.		Urządzenie musi pozwalać na przechowywanie minimum 700 kopii migawkowych jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
10.1.	Bezpieczeństwo danych	Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
10.2.		W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
10.3.		Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku oraz modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): • możliwość zdjęcia blokady przed upływem ważności danych, • brak możliwości zdjęcia blokady przed upływem ważności danych (tryb „compliance”, wymagane wsparcie dla norm SEC 17a-4(f) oraz ISO Standard 15489-1) – wymagane oficjalne wsparcie (potwierdzone na stronie producenta oprogramowania) przez producenta oprogramowania backupowego
10.4.		Wymagana funkcjonalność replikacji oraz blokady WORM muszą oficjalnie wspierać możliwość replikacji danych objętych blokadą, proces replikacji powinien zakończyć się zainicjalizowaniem blokady danych zreplikowanych w takim trybie jaki był użyty w przypadku danych oryginalnych.
10.5.		Blokada WORM musi być zintegrowana z oferowaną aplikacją backupową, musi umożliwiać: • uruchomienie blokady WORM dla określonych danych z poziomu aplikacji backupowej, • określenie/wymuszenie czasu blokady z poziomu aplikacji backupowej, • raportowanie - danych zabezpieczonych przed usunięciem wymaganą blokadą WORM z poziomu aplikacji backupowej.
10.6.		Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności snapshot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.
10.7.		Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backupowych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność.

		Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
11.1.	Czyszczenie danych	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia.
11.2.		Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
11.3.		Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
11.4.		Urządzenie musi umożliwiać systemowo (tj. poprzez wbudowaną funkcjonalność) realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
11.5.		Wymagana możliwość zdefiniowania harmonogramu według którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
11.6.		Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu „dobre praktyki" publikowanej przez producenta).
11.7.		Urządzenie musi umożliwiać uruchamianie procedury sanitacji zgodnej z normą NIST 800-88a (wytyczna 800-88r1, procedura „purge") lub równoważną.
12.1.	Zarządzanie	Urządzenie musi mieć możliwość zarządzania poprzez • interfejs graficzny dostępny z przeglądarki internetowej, • linię komend (CLI) dostępną z poziomu SSH (secure shell)
12.2.		Możliwość grupowania deduplikatorów w grupy, w których można wspólnie zarządzać urządzeniami oraz definiować równoważenie zajętości miejsca między urządzeniami celem usprawnienia późniejszego odzyskiwania danych.
13.1.	System cyber bunkra	Zaoferowane deduplikatory muszą umożliwiać rozszerzenie funkcjonalności środowiska o wdrożenie mechanizmów cyber bunkra działających zgodnie z opisem poniżej. O ile **na tym etapie dostarczenie cyber bunkra nie jest wymagane**, tak należy w ofercie podać nazwę oprogramowania (tudzież innych licencji, np. powiązanych z deduplikatorami) umożliwiających jego wdrożenie i jego metryki licencyjne.
13.2.		Środowisko cyber bunkra musi współpracować z posiadanym przez Zamawiającego oprogramowaniem: Dell EMC Networker, IBM Spectrum Protect, Commvault.
13.3.		Środowisko rozbudowane o funkcjonalność cyber bunkra musi oferować co najmniej następujące funkcjonalności: • utworzenie trzeciej warstwy danych backupowych w oparciu o dane już składowane na oferowanych deduplikatorach, gdzie komunikacja pomiędzy deduplikatorami będącymi przedmiotem zamówienia, a deduplikatorami w trzeciej (oddalonej) Lokalizacji odbywa się wyłącznie pomiędzy nimi, • zapewnienie niezmienności przechowywanych danych w okresie zaplanowanej retencji,

		• wprowadzenie analityki danych przechowywanych w cyber bunkrze pod kątem zainfekowania przez ransomware, • wprowadzenie mechanizmu raportującego umożliwiającego wskazanie danych zainfekowanych oraz danych niezainfekowanych mogących posłużyć za źródło odtwarzania systemów • utworzenie środowiska produkcyjno-testowego odizolowanego od środowiska produkcyjnego, umożliwiającego odtwarzanie oraz testowanie odtwarzanych systemów.
13.4.		System cyber bunkra musi umożliwiać replikację oraz przechowywanie całości backupów produkcyjnych pochodzących z posiadanego przez Zamawiającego oprogramowania kopii zapasowych, składowanych na oferowanych deduplikatorach.
13.5.		Deduplikator wchodzący w skład cyber bunkra musi mieć możliwość zdefiniowania blokady skasowania danych. Blokada skasowania danych musi chronić dane (podlegające blokadzie) w zdefiniowanym czasie przed usunięciem oraz modyfikacją. Wymagany tryb blokady musi działać w trybie Compliance co oznacza, że żaden użytkownik (łącznie z administratorem najwyższego poziomu urządzenia) nie może mieć możliwości zdjęcia blokady przed upływem jej retencji.
13.6.		Wymagana blokada ze względów bezpieczeństwa musi posiadać mechanizm wewnętrznego zegara, aby zapobiec skutkom potencjalnej złośliwej ingerencji w zegar systemowy, blokada musi wyeliminować możliwość zmiany aktualnej daty oraz czasu. Wymagana blokada musi blokować możliwość systemowego zniszczenia systemu plików.
13.7.		Wymagana w oferowanym deduplikatorze w/w blokada musi oficjalnie spełniać wymagania dotyczące trwałości danych, określone następującymi przepisami: • SEC 17a-4(f) • CFTC Rule 1.31b • FDA 21 CFR Part 11 • Sarbanes-Oxley Act • IRS 98025 and 97-22 • ISO Standard 15489-1 • MoREQ2010
13.8.		Deduplikator wchodzący w skład cyber bunkra musi umożliwiać bezpośrednią replikację danych z oferowanymi deduplikatorami, replikacja musi wspierać dane objęte blokadą typu Retention Lock we wszystkich dostępnych trybach, dane zreplikowane muszą automatycznie być objęte taką samą blokadą jak na urządzeniu źródłowym.
13.9.		Deduplikator wchodzący w skład cyber bunkra musi umożliwiać zestawienie równoległej jednoczesnej replikacji wielu niezależnych zasobów danych będących efektem działania zarówno wymienionych wcześniej aplikacji backupowych, jak i będących efektem backupu wbudowanymi narzędziami bazodanowymi (RMAN, Microsoft SQL Server Management Studio). W przypadku danych replikacyjnych różnych zasobów, wymagana jest możliwość: • zmiany retencji w stosunku do backupów źródłowych • niezależnego równoległego odtwarzania • założenia wymaganej blokady zapewniającej Compliance
13.10.		System cyber bunkra musi być odizolowany od środowiska produkcyjnego co oznacza między innymi, że: • deduplikator wchodzący w skład cyber bunkra nie może znajdować się w DNS / AD, nie jest używany jego FQDN,

		• w systemach po stronie produkcyjnej nie może być używany adres IP deduplikatora wchodzącego w skład cyber bunkra (wymaganie dotyczy również aplikacji backupowych), • wykluczona jest możliwość komunikacji ze strony produkcyjnej w przypadku użycia: ping, https, http, ssh czy innych standardowych metod z deduplikatorem wchodzącym w skład cyber bunkra, • komunikacji między częścią produkcyjną a deduplikatorem wchodzącym w skład cyber bunkra jest realizowana wyłącznie poprzez dedykowany protokół replikacyjny deduplikatorów.
13.11.		Cyber bunkier musi obejmować infrastrukturę automatyzującą synchronizację backupów produkcyjnych, mechanizm automatyzacji synchronizacji danych do cyber bunkra musi umożliwiać m.in.: • definicję kalendarza synchronizacji danych do cyber bunkra, wymagana częstotliwość synchronizacji w przedziale 1h do 24h z gradacją wynoszącą min. 1h, • automatyczne wyłączanie portu komunikacyjnego między deduplikatorem będącym częścią składową CB a oferowanymi deduplikatorami (poza okresem synchronizacji danych), • tworzenie do 500 snapshotów wybranego zrzutu na deduplikatorze będącym częścią składową cyber bunkra, • ręczną inicjalizację blokady (Compliance) na wybranych snapshotach, • automatyczną inicjalizację blokady na snapshotach zrzutów (Compliance) • podłączanie snapshotów do serwerów w cyber bunkra poprzez protokół NFS (sandbox) • dla danych pochodzących z oprogramowania kopii zapasowych: możliwość podłączenia snapshotów (zreplikowanych danych) do znajdującego się w cyber bunkrze systemu backupowego (tożsamego z posiadanym przez Zamawiającego) w celu umożliwienia zarządzania tymi danymi
13.12.		Zastosowany mechanizm umożliwiający analitykę składowanych w cyber bukrze danych musi: • umożliwiać jednoczesną analizę całej zawartości składowanych danych zarówno „full content" oraz analizę ich metadanych, • wykrywać infekcję typu ransomware zarówno w oparciu o metody statystyczne oraz algorytmy samouczące, • wspierać API dedykowanego protokołu deduplikacji w celu realizacji analityki inkrementalnej w przypadku backupów typu Virtual Synthetic Full.
13.13.		Cyber bunkier musi obejmować infrastrukturę umożliwiającą analizę zreplikowanych danych pod kątem ataku ransomware, wymagane funkcjonalności: • definicja kalendarza skanowania zreplikowanych danych musi być możliwa z poziomu centralnego oprogramowania cyber bunkra, • etap skanowania musi obejmować serię analiz plików oraz baz danych, zastosowany mechanizm musi rozpoznawać format popularnych plików (np. Word) a także baz danych (np. Oracle) oraz weryfikować ich poprawność pod kątem ataku ransomware, • możliwość bezpośredniego odczytu danych zreplikowanych z oferowanych deduplikatorów zapisanych w formacie używanym przez używane przez Zamawiającego oprogramowanie kopii zapasowych oraz analizy tych danych bez użycia aplikacji,

		• możliwość analizy/skanowania zawartości backupów obejmujących zasoby maszyn wirtualnych VMware pod kątem ataku ransomware, • efekty działania systemu realizującego analizę danych muszą być zapisywane do dziennika zdarzeń, • w celu optymalizacji wydajności, mechanizm skanowania powinien wykrywać dane które zmieniły się w stosunku do ich ostatnio analizowanej kopii oraz przeprowadzać analizę zmienionych/nowych części.
13.14.		Metody analizy pod kątem ataku ransomware muszą obejmować co najmniej następujące wskaźniki kompromitacji: • silne szyfrowanie z oryginalną nazwą pliku, • częściowe silne szyfrowanie z oryginalną nazwą pliku, • silne szyfrowanie RMS/MS_EFS, • silne szyfrowanie z nowym znanym rozszerzeniem, • częściowe silne szyfrowanie z nowym znanym rozszerzeniem, • silne szyfrowanie z zaciemnioną nazwą pliku, • szyfrowanie strony bazy danych, • nowe rozszerzenie pliku, • ukrycie nazwy pliku, • słabe szyfrowanie z nowym rozszerzeniem pliku, • słabe szyfrowanie z oryginalną nazwą pliku, • częściowe szyfrowanie z zaciemnioną nazwą pliku, • szyfrowanie wewnątrz z oryginalną nazwą pliku, • częściowo słabe szyfrowanie z oryginalną nazwą pliku i typem pliku, • słabe szyfrowanie z zaciemnioną nazwą pliku, • archiwum grupowe utrzymujące wymazaną oryginalną nazwę pliku, • silne szyfrowanie z nowym znanym rozszerzeniem — usuwanie zduplikowanych plików, • wypełnienie zerami z nowym znanym rozszerzeniem, • wypełnienie zerowami z oryginalną nazwą pliku, • wypełnienie zerami z zaciemnioną nazwą pliku.
14.1.	Gwarancja i wsparcie	Zamawiający wymaga min. 60 miesięcy gwarancji producenta możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.

14.2.		Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany technik Wykonawcy / Producenta z właściwym zestawem części do naprawy (potwierdzonym wstępnie na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w ciągu 4 godzin od otrzymania zgłoszenia. Naprawa ma się odbywać w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę. Dla najwyższego poziomu ważności (1) zgłoszenia (awarii krytycznej) - Zamawiający oczekuje wysłania technika serwisowego, niezależnie czy diagnostyka została już zakończona.
14.3.		Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
14.4.		Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
14.5.		Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

2. Autoryzowane szkolenia

Lp.	Opis wymagania
1.	Wykonawca dostarczy autoryzowane szkolenia producenta deduplikatorów w formie vouchera ważnego 24 miesiące od daty zakończenia Wdrożenia.
2.	W ramach autoryzowanych szkoleń zostanie zapewnione jedno podejście do egzaminu potwierdzającego wiedzę nabytą na autoryzowanym szkoleniu.
3.	Przedmiot szkolenia musi obejmować zagadnienia związane z instalacją, administracją oraz rozwiązywaniem problemów związanych z oferowanymi urządzeniami.
4.	Po zdaniu egzaminu wymienionego w punkcie 2, pracownik Wykonawcy musi posiadać uprawnienia certyfikowanego technika w zakresie administracji i utrzymania oferowanych urządzeń.

3. Projekt techniczny

Lp.	Opis wymagania
1.	Wykonawca opracuje projekt techniczny opisujący instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym.
2.	Zamawiający dostarczy dokumentację projektową będącą w jego posiadaniu i istotną dla opracowania projektu technicznego w terminie 5 dni roboczych od podpisania umowy.
3.	Projekt techniczny musi obejmować co najmniej następujące zagadnienia: • Wykaz sprzętu oraz licencji oprogramowania, • Przyjęte nazewnictwo elementów infrastruktury,

Lp.	Opis wymagania
	• Plan rozmieszczenia sprzętu w serwerowni, • Wymagania dotyczące zasilania i chłodzenia oraz wagi w poszczególnych szafach rack, • Projekt konfiguracji sprzętu oraz oprogramowania, • Projekt integracji środowiska z istniejącym otoczeniem Zamawiającego, • Projekt konfiguracji dostępu administracyjnego.
4.	Wykonawca opracuje projekt techniczny celem wdrożenia infrastruktury i oprogramowania. W ramach opracowanego dokumentu Wykonawca określi zalecenia konfiguracyjne oraz zaproponuje ewentualne zmiany w środowisku Zamawiającego.
5.	Wykonawca przygotuje scenariusze testowe dla wdrażanego środowiska. Scenariusze muszą obejmować awarię zarówno pojedynczych elementów, jak również awarię całego ośrodka.

4. Wdrożenie

Lp.	Opis wymagania
1.	Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie zaoferowane Urządzenia zgodnie z opracowanym projektem technicznym w dwóch wskazanych Lokalizacjach Zamawiającego.
2.	Wykonawca dostarczy wszystkie niezbędne elementy do wykonania prac, w szczególności kable elektryczne, patchcordy (miedziane oraz światłowodowe), organizery kabli, w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich Urządzeń.
3.	Wykonawca wykona aktualizację oprogramowania układowego na wszystkich zaoferowanych Urządzeniach oraz skonfiguruje ich interfejsy zarządzające.
4.	Wykonawca – we współpracy z Zamawiającym – dokona konfiguracji i integracji zaoferowanych Urządzeń z posiadanym przez Zamawiającego oprogramowaniem kopii zapasowych (w szczególności dokona konfiguracji deduplikacji na źródle).
5.	Wykonawca dokona hardeningu wdrażanego rozwiązania zgodnie ze standardami wskazanymi przez Zamawiającego.
6.	Wykonawca skonfiguruje wewnętrzne mechanizmy monitorowania Urządzeń, podłączy je do wskazanych przez Zamawiającego narzędzi wykorzystywanych przez zespoły NOC/SOC/SRE.
7.	W ramach Wdrożenia Wykonawca opracuje procedury eksploatacyjne dla wdrożonych komponentów. Procedury muszą obejmować wszystkie czynności, jakich należy dokonać celem monitorowania i utrzymania przedmiotu Wdrożenia w poprawnym i bezpiecznym działaniu.
8.	Przed odbiorem jakościowym Wdrożenia zostaną przeprowadzone testy zdefiniowane w projekcie technicznym. Głównym kryterium powodzenia testów będzie nieprzerwane działanie wyżej wymienionego rozwiązania w trakcie ich trwania oraz po ich zakończeniu.
9.	Końcowym wynikiem Wdrożenia będzie przygotowanie dokumentacji powykonawczej w formacie PDF, MS Word i Markdown. Formaty te są obowiązujące dla wszelkiej dokumentacji powstałej w projekcie.

5. Warsztaty

Lp.	Opis wymagania
1.	Wykonawca przeprowadzi dwudniowe Warsztaty z zakresu administracji, konfiguracji i utrzymania wdrożonych Urządzeń, przeprowadzane przez personel posiadający właściwe certyfikacje w zakresie Wdrożenia.
2.	Warsztaty dla pracowników Zamawiającego odbędą się w formie zdalnej.
3.	Program Warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne. Powinien on zawierać również informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy Warsztatów.
4.	Zamawiający zastrzega sobie prawo do korekty programu Warsztatów w uzgodnionym zakresie.