Załącznik nr 1 do Umowy nr [●]

**Opis przedmiotu zamówienia – Część II**

**[ECS]**

1. **Przedmiot zamówienia**
   1. Przedmiotem zamówienia jest dostawa 12 szt. węzłów Elastic Cloud Storage w skrócie ECS (dalej łącznie „Urządzenia”) spełniających funkcjonalność Direct Read Support dla Cloud Tier potwierdzoną w matrycy kompatybilności z urządzeniami Data Domain - w ramach modernizacji środowiska kopii zapasowych opisanego w Tabeli 1a poniżej, zgodnie ze specyfikacją zawartą w Tabeli 1 i Tabeli 2 poniżej, co obejmuje również zadania, o których mowa w pkt. 1.8 poniżej, z zachowaniem pełnego wsparcia oraz kompatybilności z urządzeniami oraz oprogramowaniem aktualnie zainstalowanym w środowisku kopii zapasowych, tj. Data Domain oraz Data Protection Suite for Vmware pochodzącymi od Dell Technologies.
   2. Urządzenia muszą pochodzić z oficjalnego kanału sprzedaży ich producenta.
   3. Urządzenia muszą być fabrycznie nowe tj. nieużywane i wyprodukowane nie wcześniej niż 6 miesięcy przed terminem dostawy, kompletne, wolne od wad, bez śladów używania i bez uszkodzeń.
   4. Urządzenia muszą być oryginalne, przy czym pod pojęciem oryginalny należy rozumieć sprzęt dopuszczony do obrotu na terenie Rzeczpospolitej Polskiej, wprowadzony na rynek zgodnie z przepisami Ustawy o zużytym sprzęcie elektrycznym i elektronicznym z dnia 11 września 2015 r. (t.j. Dz. U. z 2022 r. poz. 1622), posiadający wymagane prawem deklaracje zgodności, jak również instrukcje obsługi w języku polskim.
   5. W chwili dostarczenia (do czasu rozpakowania na potrzeby montażu), Urządzenia muszą znajdować się w opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, posiadać zabezpieczenia (o ile zostały zastosowane przez producenta), oznaczenie CE oraz znaki identyfikujące Urządzenia, a w szczególności znak towarowy lub markę producenta Urządzeń.
   6. Realizacja zamówienia nie może spowodować utraty gwarancji udzielonych na środowisko kopii zapasowych aktualnie eksploatowane przez Zamawiającego (infrastrukturę, w tym dyski i inne podzespoły, oraz oprogramowanie sprzętowe). Konsekwentnie, Wykonawca zobowiązany jest przy realizacji zamówienia przestrzegać zasad i ograniczeń, wynikających z warunków gwarancyjnych dotyczących sprzętu i oprogramowania opublikowanych przez producenta środowiska kopii zapasowych aktualnie pod adresem <https://www.dell.com/support/contents/pl-pl/article/warranty/dell-emc-warranty>
   7. Wykonawca zapewni, aby Urządzenia oraz sposób ich montażu, spełniały wymogi bezpieczeństwa określone przez przepisy Unii Europejskiej dotyczące bezpieczeństwa określonego produktu (Conformité Européenne) oraz szczegółowe wymagania dotyczące bezpieczeństwa produktu określone przepisami polskimi, a w ich braku, wymogi dobrowolnych norm krajowych państw UE innych niż normy uznane przez KE, Polskich Norm, zaleceń KE, zasad dobrej praktyki w zakresie bezpieczeństwa produktu obowiązujących w danym sektorze, aktualnego stanu wiedzy i techniki lub uzasadnionych oczekiwań użytkowników w zakresie bezpieczeństwa.
   8. W ramach dostawy Urządzeń, Wykonawca wykona:
      1. montaż Urządzeń zgodnie z ustaleniami w trybie roboczym;
      2. montaż (instalację fizyczną) w szafach RACK zgodnie z ustaleniami w trybie roboczym;
      3. aktywację oprogramowania układowego (ang. firmware) i narzędziowego (o ile okaże się wskazana);
      4. uruchomienie środowiska po modernizacji;
      5. konfigurację sprzętowo-systemową środowiska kopii zapasowych po modernizacji (o ile okaże się wskazana);
      6. dokumentację powdrożeniową, zawierającą co najmniej następujące informacje:
         1. konfiguracja środowiska kopii zapasowych przed i po rozbudowie.
   9. Prace, o których mowa w pkt 1.8, muszą zostać przeprowadzone zgodnie z zasadami sztuki, zgodnie z wytycznymi wynikającymi z zawartych przez Zamawiającego umów serwisowych dotyczących eksploatowanego sprzętu, a przy tym w sposób bezpieczny, niezagrażający utracie danych i gwarantujący nieprzerwane funkcjonowanie systemu (nieustanna praca w trybie biznesowym). Dokładny przebieg realizacji tych zadań wymaga uzgodnienia z Zamawiającym.
   10. Montaż (instalacja fizyczna), uruchomienie i konfiguracja muszą zostać wykonane zgodnie z rekomendacjami producenta środowiska kopii zapasowych Dell Technologies posiadanego przez Zamawiającego, a przy tym bez wpływu na działające środowiska i bez powodowania jakichkolwiek przerw czy opóźnień w dostępie do danych.
   11. Wszystkie elementy dodatkowe wymagane do montażu (instalacji fizycznej) Urządzeń (śrubki, kable itp.) oraz do ich uruchomienia oraz konfiguracji środowiska kopii zapasowych muszą zostać dostarczone przez Wykonawcę w ramach zamówienia.
   12. Zbędne (np. trwale uszkodzone) dyski pozostaną w miejscu realizacji zamówienia.
   13. Wykonawca traktowany jest jako wytwórca odpadów powstałych w toku realizacji zamówienia i utylizuje je na własny koszt i ryzyko, zgodnie z właściwymi przepisami.
   14. Wytyczne i rekomendacje, o których mowa w pkt 1.9 i 1.10 zostaną przekazane Wykonawcy w trybie roboczym (w toku realizacji zamówienia).
2. **Termin realizacji dostawy** 
   1. Wykonawca dostarczy Urządzenia jednorazowo, nie później niż 45 dni od zawarcia Umowy.
   2. O planowanym terminie dostarczenia Urządzeń Wykonawca poinformuje Zamawiającego z wyprzedzeniem co najmniej 3 dni roboczych.
   3. Czynności, o których mowa w pkt 1.8, z wyjątkiem przedmiotu zamówienia, o którym mowa w pkt 1.8.6, muszą zostać wykonane w ciągu 5 dni od dnia dostarczenia Urządzeń, w godzinach 08.00-16.00.
   4. Dokumentacja powdrożeniowa (pkt 1.8.6) zostanie opracowana i dostarczona Zamawiającemu nie później niż w ciągu 7 dni od daty zakończenia montażu (instalacji fizycznej) i uruchomienia Urządzeń, aktywacji oprogramowania oraz konfiguracji środowiska kopii zapasowych, potwierdzonych pozytywną weryfikacją przez Zamawiającego, w oryginale (2 egz.) oraz w postaci elektronicznej (plik .doc lub .docx).
   5. Nie później niż w dacie montażu Urządzeń, Wykonawca zobowiązany jest przekazać Zamawiającemu wystawione przez producenta Urządzeń instrukcje ich użytkowania, atesty, deklaracje zgodności, itp.
   6. W braku odmiennego uzgodnienia Stron, przyjmuje się, że termin realizacji czynności w ramach wsparcia producenta oprogramowania wynosi 5 (pięć) dni roboczych (przez „dzień roboczy” rozumie się dzień niebędący dniem wolnym od pracy ani sobotą) od zgłoszenia przez Zamawiającego.
3. **Miejsce realizacji dostawy** 
   1. Miejscem realizacji przedmiotu zamówienia jest obiekt (jeden bądź dwa) zlokalizowany na terenie woj. mazowieckiego. Zamawiający, w formie pisemnej lub w formie elektronicznej, wskaże adres tego miejsca (jedno bądź dwa), po podpisaniu Umowy.
   2. Zamawiający zastrzega sobie możliwość zmiany miejsca realizacji podanego w zawiadomieniu, o którym mowa w pkt 3.1 na inną lokalizację w granicach tego samego województwa, za zawiadomieniem Wykonawcy w formie pisemnej lub w formie elektronicznej z wyprzedzeniem co najmniej 5 dni.
   3. Zamawiający zastrzega sobie prawo do przeniesienia Urządzeń do innej lokalizacji, bez utraty uprawnień wynikających z gwarancji i rękojmi.
   4. Naprawy Urządzeń w ramach gwarancji i rękojmi, będą dokonywane w miejscu ich eksploatacji, wynikającym z pkt 3.1-3.3. W przypadku niemożności dokonania naprawy w miejscu eksploatacji Urządzeń, Wykonawca na swój koszt i ryzyko zapewnia dostarczenie i odbiór Urządzenia do/z autoryzowanego punktu serwisowego.
4. **Sposób realizacji dostawy** 
   1. Dostawa urządzeń, w tym w ramach wymiany serwisowej, obejmuje każdorazowo również transport z wniesieniem oraz montaż (instalację fizyczną), uruchomienie i konfigurację tych urządzeń w lokalizacji.
   2. Dokumentacja zostanie sporządzona w języku polskim.
   3. Komunikacja oraz wszelka korespondencja pomiędzy Stronami będzie odbywała się w języku polskim.
   4. W ramach realizacji zamówienia, Wykonawca przeniesie na Zamawiającego prawa autorskie majątkowe do dostarczonych lub wytworzonych utworów w zakresie wskazanym w § 8 Umowy.
5. **Serwis gwarancyjny**
   1. Wykonawca udzieli Zamawiającemu rękojmi za wady dostarczonych rzeczy, usług i dzieła (utworów) oraz gwarancji na prawidłowe działanie Urządzeń i oprogramowania, co do ich jakości oraz zgodności z dokumentacją techniczną i dokumentacją powdrożeniową, stosownie do § 9 Umowy.
   2. Wykonawca opracuje i przekaże Zamawiającemu nie później niż w dniu podpisania protokołu odbioru przedmiotu zamówienia (dostawy), w formie pisemnej i w postaci elektronicznej, dokument pt. „Instrukcja zgłaszania, obsługi i eskalacji zgłoszeń serwisu gwarancyjnego”, zawierający:
      1. instrukcje zgłaszania awarii, w tym formularz – Zgłoszenia gwarancyjnego;
      2. procedury eskalacyjne (pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub reakcji na zgłoszenie);
      3. dane podmiotu świadczącego usługi gwarancyjne - adresy, numery telefonów i faksów, adresy poczty elektronicznej;
      4. instrukcje dotyczące przeglądania statusu Umowy oraz urządzeń nią objętych;
      5. wzór Raportu z naprawy urządzenia.

Instrukcje i procedury, o których mowa powyżej, nie mogą być sprzeczne lub niezgodne z postanowieniami Umowy.

Zmiana dokumentów wymienionych w niniejszym punkcie wymaga powiadomienia Zamawiającego w formie pisemnej albo w formie elektronicznej.

Wykonawca zobowiązuje się wdrożyć i stosować przez cały okres obowiązywania Umowy powyższe procedury i instrukcje.

Przekazane przez Wykonawcę procedury i instrukcje podlegają akceptacji Zamawiającego. Zamawiający może zgłosić uwagi i poprawki do instrukcji i procedur przekazanych przez Wykonawcę, a Wykonawca jest zobowiązany do ich uwzględnienia i przedstawienia do ponownej akceptacji przez Zamawiającego.

* 1. Zgłoszenie awarii urządzeń objętych gwarancją może być dokonywane w postaci: zgłoszenia telefonicznego, za pomocą faksu, z wykorzystaniem serwisu www udostępnionego przez Wykonawcę, za pomocą poczty elektronicznej oraz zgłoszeń generowanych automatycznie przez system monitoringu eksploatowanych urządzeń.
  2. Wykonawca będzie przyjmował zgłoszenia awarii całodobowo (24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku).
  3. Konsultacje techniczne w ramach serwisu gwarancyjnego mogą być przeprowadzone pomiędzy Wykonawcą a Zamawiającym osobiście, telefonicznie lub za pomocą poczty elektronicznej.
  4. Wykonawca jest zobowiązany do potwierdzenia przyjęcia zgłoszenia awarii (lub konsultacji technicznych) w terminie do 60 minut od jego zgłoszenia na adres poczty elektronicznej [popd@ms.gov.pl](mailto:popd@ms.gov.pl) lub telefonicznie – na numer podany podczas rejestracji zgłoszenia, niezwłocznie przesyłając potwierdzenie mailem na powyższy adres mailowy, przy czym za chwilę potwierdzenia przyjęcia zgłoszenia uważa się moment potwierdzenia telefonicznego. W przypadku braku potwierdzenia, po upływie 60 minut od zgłoszenia awarii przez Zamawiającego, Zamawiający wdroży procedurę eskalacji zgłoszenia, o której mowa w pkt. 5.2.2.
  5. Wykonawca zobowiązany jest do zapewnienia procedury eskalacyjnych zgłoszeń zawierających co najmniej dodatkowe dwa numery telefonów. Pod pojęciem procedury eskalacji Zamawiający rozumie tryb postępowania stron w sytuacji braku realizacji zgłoszenia lub reakcji na zgłoszenie, na zasadach określonych w procedurze eskalacji zgłoszenia, o której mowa w pkt. 5.2.2.
  6. Wykonawca zobowiązany jest do zapewnienia Zamawiającemu możliwości bieżącego śledzenia statusu zgłoszenia za pośrednictwem co najmniej strony www – Wykonawca przekaże Zamawiającemu login i hasło nie później niż w dniu podpisania Protokołu Odbioru.
  7. Wykonawca zapewni Zamawiającemu dostęp do monitorowania statusu zgłoszeń gwarancyjnych w systemie producenta.
  8. Zamawiający wymaga zapewnienia ciągłości usług serwisu gwarancyjnego.
  9. Zgłoszenia awarii będą realizowane w następujący sposób:
     1. Zgłoszenie o priorytecie krytycznym tj. nieprawidłowe działanie Urządzeń, powodujące albo całkowity brak możliwości korzystania z Urządzeń albo takie ograniczenie możliwości korzystania z Urządzeń, że przestają one spełniać swoje podstawowe funkcje – czas reakcji do 24 godzin serwisowych od chwili zgłoszenia, czas przywrócenia funkcjonalności do [●] godzin serwisowych od chwili zgłoszenia (zgodnie z ofertą Wykonawcy, nie dłużej jednak niż do 48 godzin serwisowych).
     2. Zgłoszenie o priorytecie niekrytycznym tj. inne niż krytyczne, np. zmniejszenie wydajności Urządzenia – czas reakcji nie później niż w następnym dniu roboczym od dnia zgłoszenia, czas przywrócenia funkcjonalności do 96 godzin serwisowych od chwili zgłoszenia.
  10. Wykonawca zobowiązany jest do realizowania czasów reakcji i napraw w godzinach między 7.00 a 17.00 od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy (godziny serwisowe).
  11. W przypadku, gdy Wykonawca nie wykona obowiązku wynikającego z pkt. 5.11:
      1. Zamawiający ma prawo wypożyczyć, zainstalować i uruchomić na koszt Wykonawcy u dowolnego innego dostawcy urządzenie zastępcze, zachowując jednocześnie prawo do kary umownej i odszkodowania.
      2. Zamawiający ma prawo zlecić dowolnemu innemu dostawcy naprawę urządzenia, a kosztami naprawy obciążyć Wykonawcę zachowując jednocześnie prawo do kary umownej i odszkodowania.
  12. W przypadku wystąpienia okoliczności opisanych w pkt 5.13.1 lub 5.13.2 Zamawiający nie traci prawa do gwarancji.
  13. W ramach usunięcia awarii Urządzenia, Zamawiający dopuszcza możliwość wymiany przez Wykonawcę po uzgodnieniu z Zamawiającym poszczególnych elementów i podzespołów Urządzenia lub całego Urządzenia na nowe takie samo lub inne, o co najmniej takich samych parametrach, funkcjonalności i standardzie.
  14. W przypadku, gdy z uwagi na awarię Urządzenia Wykonawca zapewnił urządzenie zastępcze, a naprawa dotkniętego awarią Urządzenia trwa dłużej niż 6 tygodni lub gdy ten sam element/podzespół/część Urządzenia będzie naprawiany trzykrotnie w okresie gwarancyjnym i nastąpi kolejna (czwarta) awaria, Zamawiający może żądać od Wykonawcy wymiany Urządzenia na nowe, takie samo lub inne, uzgodnione z Zamawiającym, w terminie 30 dni od zgłoszenie takiego żądania przez Zamawiającego, o co najmniej takich samych parametrach, funkcjonalności i standardzie. Dostarczone w ramach wymiany Urządzenie musi być fabrycznie nowe tj. wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą, wolne od wad, bez śladów używania i bez uszkodzeń, wprowadzone na rynek zgodnie z przepisami Ustawy o zużytym sprzęcie elektrycznym i elektronicznym z dnia 11 września 2015 r. (t.j. Dz. U. z 2022 r. poz. 1622) dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych, zabezpieczających przed uszkodzeniem w trakcie transportu i składowania. W przypadku wymiany Urządzenia na nowe, Wykonawca sporządzi protokół z wymiany.
  15. Wykonawca każdorazowo dostarczy Zamawiającemu sprawozdanie (raport) z naprawy Urządzenia, zawierający datę i godzinę zgłoszenia, informację co było przedmiotem naprawy. W przypadku przekroczenia limitów czasu usunięcia awarii, wynikających z pkt. 5.11, Wykonawca uwzględni w rzeczonym raporcie stosowne informacje w tym względzie.
  16. W okresie trwania gwarancji i rękojmi, Zamawiający ma prawo do instalowania, wymiany standardowych kart rozszerzeń/modułów i podzespołów (np. modułów optycznych itp.) oraz rozbudowy poszczególnych sprzętów/urządzeń oraz instalacji pobranych poprawek, aktualizacji, oprogramowania narzędziowego i nowych wersji systemu operacyjnego sprzętów/urządzeń (firmware) zgodnie z zasadami sztuki w tym zakresie przez wykwalifikowany personel Zamawiającego lub podmiotu zewnętrznego, któremu zleci te prace Zamawiający.
  17. W przypadku awarii powodującej konieczność wymiany dysku lub innego nośnika danych, uszkodzone nośniki pozostają w gestii Zamawiającego.

**Tabela 1. Podzespoły środowiska kopii zapasowych aktualnie eksploatowanego przez Zamawiającego, podlegające wymianie w ramach niniejszego zamówienia**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **typ produktu** | **numer seryjny** | **aktualna przestrzeń dyskowa (opis)** | **komentarz** |
| 1 | ECS | CKM00182401616 | 5 węzłów gen.2 | wymiana na 6 nowych węzłów |
| 2 | ECS | CKM00182601672 | 5 węzłów gen.2 | wymiana na 6 nowych węzłów |

**Tabela 1a. Podzespoły środowiska kopii zapasowych aktualnie eksploatowanego przez Zamawiającego.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **typ produktu** | **numer seryjny** | **aktualna przestrzeń dyskowa (opis)** |
| 1 | Data Domain DD9400 | CKM01214706140 | 240TB OP + 960TB AT, rozmieszczone w 3 półkach DS60 |
| 2 | Data Domain DD9400 | CKM01214706143 | 240TB OP + 960TB AT, rozmieszczone w 3 półkach DS60 |
| 3 | ECS | CKM00182401616 | 6 węzłów |
| 4 | ECS | CKM00182601672 | 6 węzłów |

**Tabela 2. Specyfikacja Urządzeń**

Zamawiający aktualnie eksploatuje środowisko kopii zapasowych (Data Center) marki Dell Technologies, w którym dane składowane są bezpośrednio w trybie deduplikacji na źródle na urządzeniach DELL Technologies Data Domain DD9400 oraz ECS, w oparciu o oprogramowanie DELL Technologies pozwalające aktualnie na backup i archiwizację oraz zarządzanie danymi w ramach środowiska kopii zapasowych liczącym w sumie 300 CPU – pakiet Data Protection Suite for Vmware (DPS4VM), w skład którego wchodzą aplikacje:

* NetWorker;
* Data Protection Central;
* Data Protection Advisor;
* DP Search;
* Cloudboost.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **produkt** | **wymagania funkcjonalne (minimalne)** | **liczba szt.** | **zastosowanie** |
| 1. | węzły ECS | Dostarczane rozwiązanie (Elastic Cloud Storage) musi być obecne na rynku od co najmniej 5 lat oraz musi współpracować z posiadanym przez Zamawiającego urządzeniami Data Domain i umożliwiać rozbudowę ich pojemności w ramach funkcjonalności Cloud Tier.  Rozwiązanie musi spełniać funkcjonalność Direct Read Support dla funkcjonalności Cloud Tier potwierdzone w matrycy kompatybilności z urządzeniami Data Domain.  Dostarczane rozwiązanie musi być produktem rozpoznawalnym na rynku, co oznacza, że powinno być wymieniane w raportach niezależnych organizacji, takich jak Gartner, IDC, Gigaom lub ESG (Enterprise Strategy Group).Oferowane rozwiązanie musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności.  Rozwiązanie musi umożliwiać dostępu do danych co najmniej za pomocą następujących interfejsów i protokołów: Amazon S3, OpenStack Swift oraz NFS. Jeżeli wykorzystanie któregokolwiek z wymienionych protokołów wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem.  Rozwiązanie musi posiadać możliwość integracji z aplikacjami za pomocą protokołu HDFS.  System musi umożliwiać dostęp do tych samych danych przy pomocy wszystkich wymaganych protokołów (Amazon S3, OpenStack Swift, NFS, HDFS).  Rozwiązanie dodatkowo powinno posiadać możliwość dostępu do danych za pomocą protokołów Centera CAS oraz Atmos.  Dane w obiektowym systemie składowania danych będącym przedmiotem zapytania muszą być składowane jako obiekty składające się z danych oraz opisujących je metadanych. Metadane nie mogą być składowane w wydzielonej bazie danych, a replikacja danych (obiektów) obywa się spójnie z metadanymi.  Dla protokołu S3 rozwiązanie musi posiadać wbudowany mechanizm indeksowania i przeszukiwania metadanych. Musi istnieć możliwość wyszukiwania w oparciu o wewnętrzną wyszukiwarkę lub interfejs API pozwalający na integrację silnika wyszukiwania z własną aplikacją.  Rozwiązanie musi posiadać możliwość zdefiniowania kluczy metadanych do indeksowania.  Per Bucket musi istnieć możliwość zdefiniowania min. 30 kluczy do indeksowania.  Rozwiązanie powinno posiadać wbudowany mechanizm wersjonowania obiektów w przypadku wykorzystania protokołu S3.  Rozwiązanie musi umożliwiać zarządzanie listami kontroli dostępu ACL oraz politykami dostępu do Bucket'ów (Bucket Policy), przy pomocy których można definiować uprawnienia przyznawane użytkownikom.  Urządzenie powinno wspierać autentykację przy pomocy mechanizmu IAM (Identity and Access Management).  Platforma powinna być zbudowana w architekturze scale-out (skalowalnej horyzontalnie).  Wymagana pojemność musi być dostarczona, zainstalowana i skonfigurowana do pracy w dwóch ośrodkach przetwarzania danych. Każdy obiekt docelowo powinien być przechowywany w obu ośrodkach, a rozwiązanie powinno być odporne na awarię dowolnego z tych ośrodków tzn. taka awaria nie może prowadzić do utraty pojemności, utraty danych, ani do utraty dostępu do nich.  Dostarczony sprzęt w każdej lokalizacji powinien posiadać pojemność przynajmniej 700 TB netto, - bez wykorzystania mechanizmów redukcji danych i po zastosowaniu wymaganej protekcji.  Każda lokalizacja powinna być zbudowana z przynajmniej 6 węzłów/kontrolerów.  Rozwiązanie powinno umożliwiać skalowanie poprzez dokładanie kolejnych kontrolerów i/lub dysków. Wymagana jest skalowalność do pojemności min 100PB. Rozbudowa rozwiązania powinna być bezprzerwowa.  Wymagana pojemność musi być dostarczona na dyskach twardych znajdujących się wewnątrz węzłów rozwiązania. Nie są dopuszczalne rozwiązania oparte o taśmy, czy platformy chmurowe.  Dopuszczalne są dyski typu SATA lub NL-SAS nie większej pojemności niż 8TB.  Rozwiązanie musi być wyposażone w pamięć flash (w postaci dysków SSD lub modułów flash) na potrzeby akceleracji i buforowania metadanych. Wymagana jest pojemność min. 960GB per węzeł.  Dane muszą być chronione przy pomocy kodowania nadmiarowych (Erasure Coding) na wewnętrznych dyskach kontrolerów. Rozwiązanie nie dopuszcza stosowania struktur typu RAID czy LUN wymagających dodatkowego administrowania.  Przestrzeń służąca do przechowywania danych powinna być skonfigurowana tak, aby była odporna na jednoczesną awarię co najmniej 2 dowolnych dysków twardych lub kontrolerów (tzn. taka awaria nie powinna prowadzić do utraty danych).  Dostęp do rozwiązania powinien być realizowany za pomocą protokołu Ethernet oraz interfejsów 10Gb lub 25Gb.  W przypadku, gdy system wymaga przełączników na potrzeby wewnętrznej i/lub zewnętrznej komunikacji, należy zapewnić redundantne przełączniki LAN 10Gb lub 25Gb z odpowiednią ilością portów. Przełączniki powinny pochodzić od tego samego producenta, co reszta rozwiązania.  Urządzenie nie może posiadać pojedynczego punktu awarii, tzn. wszystkie jego elementy muszą być redundantne, a jego architektura musi zapewniać odporność na awarię w obrębie poszczególnych grup elementów, przynajmniej w zakresie dysków, interfejsów dostępowych, kontrolerów, zasilaczy i wentylatorów.  Rozwiązanie musi mieć możliwość podłączenia go do centrum serwisowego producenta w celu zdalnego monitorowania poprawności funkcjonowania komponentów rozwiązania.  Ze względu na wysoką dostępność, oferowane urządzenie musi umożliwiać dostęp do danych bezpośrednio przez wszystkie dostarczone kontrolery (t.j. bez wydzielonych kontrolerów dostępowych, management'owych, storage'owych itd)  Oferowane rozwiązanie musi być oparte o kontrolery o wysokości nie większej niż 2RU  Rozwiązanie powinno umożliwiać zapisanie przynamniej 10 mld obiektów bez konieczności rozbudowy czy dodawania kontrolerów.  Urządzenie musi umożliwiać replikację w technologii geograficznie rozproszonego klastra pracującego w trybie active/active, tzn. te same dane (obiekty) powinny być dostępne w trybie odczyt/zapis w obu ośrodkach jednocześnie.  W replikacji active/active system musi mieć możliwość pracy w trybie tzw. "strong consistency" tzn. powinien zwracać najbardziej aktualną wersję obiektu, niezależnie od tego, do którego ośrodka trafi zapytanie.  Replikacja musi odbywać się w ramach szyfrowanego kanału. Funkcjonalność szyfrowania powinna być wspierana przez platformę obiektową.  Przynajmniej dla protokołów NFS, Centera CAS oraz S3 system musi zapewniać i gwarantować niezmienność składowanych w nim obiektów poprzez wykorzystanie wbudowanej funkcjonalności WORM (Write Once Read Many). Funkcjonalność WORM musi być realizowana wewnątrz dostarczonego gotowego rozwiązania sprzętowego w jego oprogramowaniu systemowym.  Rozwiązanie musi posiadać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu.  Rozwiązanie musi pozwalać na zdefiniowanie partycji, w których istnieje możliwość usuwania danych przed upływem retencji oraz partycji (tzw. tryb Enterprise), w których usuwanie danych przed upływem retencji jest niemożliwe - również przez operatora/administratora platformy (tzw. tryb Compliance). Rozwiązanie powinno pozwalać na definiowanie i uruchamianie jednocześnie obydwu typów partycji. Jeżeli ta funkcjonalność wymaga dodatkowej licencji, należy ją dostarczyć.  Rozwiązanie natywnie (tzn. bez hostów pośredniczących) powinno wspierać replikację do innych targetów S3 (np. Bucket S3 w Amazon AWS)  Wymagana wsparcie dla S3 ObjectLock.  Dla funkcjonalności WORM urządzenie musi spełniać wymagania standardu SEC 17-a4 oraz FIPS.  Rozwiązanie musi posiadać możliwość tworzenie logicznie odseparowanych obszarów tzw. „MULTI-TENANCY”. Wymagana jest możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, polityki składowania danych, monitorowanie wykorzystania) tak tworzonymi obszarami.  Zamawiający wymaga, aby dostarczone rozwiązanie posiadało możliwość zdefiniowania co najmniej 1000 logicznych partycji ("tennant'ów").  Musi istnieć możliwość mapowania zasobów do różnych zastosowań w taki sposób, aby dla każdego z nich możliwe było definiowanie różnych i niezależnych parametrów i kryteriów składowania danych w tym, co najmniej: retencji, quoty, indeksowania i replikacji.  Wymagana jest możliwość autentykacji z użyciem AD/LDAP.  Rozwiązanie musi posiadać swoje własne wbudowane mechanizmy weryfikacji integralności danych np przy pomocy sum kontrolnych składowanych obiektów.  Rozwiązanie musi posiadać wbudowane mechanizmy redukcji danych, w tym co najmniej kompresję danych. W przypadku braku tej funkcjonalności, należy dostarczyć 100% więcej pojemności.  Rozwiązanie musi posiadać funkcjonalność szyfrowania danych przechowywanych na dyskach obiektowego magazynu składowania danych. Wymagane jest użycie algorytmu min. AES-256 lub równoważnego. Jeżeli wymagana jest licencja, należy ją dostarczyć. Urządzenie musi posiadać wbudowany menedżer kluczy szyfrujących, jak i umożliwiać integrację z zewnętrzym menedżerem kluczy za pomocą protokołu KMIP.  Wymagane jest wsparcie dla komend API S3 Select.  Rozwiązanie powinno umożliwiać rozbudowę o narzędzia do wykrywania i automatycznego reagowania na ataki typu Ransomware.  Rozwiązanie musi umożlwiać:  - zarządzanie co najmniej poprzez graficzny interfejs użytkownika oraz poprzez API;  - automatyczny monitoring obejmujący m.in.: utylizację zasobów on-line (w tym CPU, pamięć, sieć), zajętość miejsca, transfery, czy ilość operacji;  - tworzenie alertów i powiadomień dot. stanu SYSTEMU, automatyczne przesyłanie ich poprzez e-mail | 12 | ECS |