Załącznik nr 1 do SIWZ

Opis przedmiotu zamówienia

LP	Nazwa	Ilość	Cena jednostkowa brutto	Wartość brutto
1.	Rozbudowa systemu kopii bezpieczeństwa systemów teleinformatycznych	1		
			SUMA :	

Załącznik nr 1 do SIWZ

LP	Nazwa	Nazwa producenta i oznaczenie typu proponowanych urządzeń/oprogramowania
1.	Rozbudowa systemu kopii bezpieczeństwa systemów teleinformatycznych	Rozwiązanie: a) Producent: …… b) Model: …… c) Oznaczenie, które pozwoli na jednoznaczną identyfikację produktu (np. symbol, kod produktu itd.) …… …… Sprzęt (w tym serwery i urządzenia przechowujące dane): a) Producent: …… b) Model: …… c) Oznaczenie, które pozwoli na jednoznaczną identyfikację produktu (np. symbol, kod produktu itd.) …… …… Oprogramowanie: a) Producent: …… b) Model: …… c) Oznaczenie, które pozwoli na jednoznaczną identyfikację produktu (np. symbol, kod produktu itd.) …… …… Licencje: a) Producent: …… b) Model: …… c) Oznaczenie, które pozwoli na jednoznaczną identyfikację produktu (np. symbol, kod produktu itd.) …… ……

UWAGA: W poniższych tabelach należy wpisać w ostatniej kolumnie w wykropkowanych miejscach dokładne wartości oferowanych parametrów spełniających minimalne wymagania, a w miejscach gdzie wymagane jest spełnienie określonych cech, skreślić niepotrzebne „Nie spełnia” lub „Spełnia”. Należy wpisać producenta, model oraz inne oznaczenie jednoznacznie identyfikujące proponowane urządzenie lub oprogramowanie.

W przypadku zaproponowania rozwiązań na podstawie udzielonych odpowiedzi do pytań oferentów dot. OPZ zamawiający zaleca odwołanie się do konkretnej odpowiedzi.

Załącznik nr 1 do SIWZ

1. Rozbudowa systemu kopii bezpieczeństwa systemów teleinformatycznych

……

Nazwa producenta i oznaczenie typu proponowanych urządzeń (należy uwzględnić i wymienić urządzenia wchodzące w skład zestawu) oraz oprogramowanie

1. Przedmiotem zamówienia jest rozbudowa posiadanego przez Zamawiającego systemu kopii bezpieczeństwa systemów teleinformatycznych opartego o urządzenie EMC AVAMAR M2400 poprzez dostarczenie i wdrożenie urządzenia przechowującego dane oraz niezbędnych licencji. Wymagane jest wykonanie dokumentacji powykonawczej wraz z instruktażem stanowiskowym 3 osób z dostarczonego rozwiązania w ilości min. 16 godz.

2. Zamawiający posiada i użytkuje system kopii bezpieczeństwa w oparciu o oprogramowanie EMC AVAMAR o nr identyfikacyjnym 1409132401001E67A0AB0A oraz fizyczny appliance EMC M2400, o numerze seryjnym FC6AV142900022. Posiadany system kopii bezpieczeństwa objęty jest 5-letnią gwarancją dostawcy systemu, licząc od dnia 19.12.2014 r.

3. Zamawiający wymaga rozbudowania istniejącego systemu kopii bezpieczeństwa systemów teleinformatycznych poprzez:

   a) wydłużenie wsparcia serwisowego i gwarancyjnego posiadanego systemu kopii bezpieczeństwa wymienionego w pkt. 2, do maksymalnego terminu wsparcia producenta (end-of-support) licząc od dnia końca gwarancji określonej w pkt. 2.

   b) zwiększenie przestrzeni składowania danych posiadanego systemu kopii bezpieczeństwa o minimum **70** TB (+/- 1TB) przestrzeni użytkowej do składowania danych poprzez dołożenie fizycznego urządzenia. Rozbudowa do większej pojemności powinna być możliwa poprzez bezpośrednie dołożenie kolejnych półek z dyskami oraz odpowiednich licencji. Rozbudowa nie może być realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń.

   c) zwiększenie ilości posiadanych licencji.

4. Sumaryczna ilość dostarczonych w ramach rozbudowy licencji dla urządzeń wyspecyfikowanych w pkt. 3b i 3c musi pozwalać na przechowywanie min. 10 TB deduplikatów danych.

5. Sumaryczna ilość licencji całego systemu kopii bezpieczeństwa (suma z pkt. 3a, 3b i 3c) musi pozwalać na przechowywanie min. 15 TB deduplikatów

danych.

6. Rozwiązanie opisane w pkt 3b musi być skalowalne do przestrzeni użytkowej minimum 150 TB (+/- 10 TB) w ramach tego samego urządzenia, rozbudowa do wymaganej pojemności musi być możliwa poprzez dołożenie kolejnych dysków lub kolejnych półek z dyskami oraz odpowiednich licencji, rozbudowa nie może być realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń.
7. Rozwiązanie musi mieć możliwość migracji licencji z appliance'u fizycznego wymienionego w pkt 3a do rozwiązania wymienionego w pkt 4, uzyskując pojemność z pkt 5. Musi być możliwość migracji cząstkowej liczby licencji z urządzenia opisanego w pkt 3a
8. Rozwiązanie musi mieć możliwość wykonywania kopii bezpieczeństwa i ich odtwarzania w obrębie samego urządzenia będącego appliance'm fizycznym opisanym w pkt. 3a jak również musi mieć możliwość rozszerzenia pojemności urządzenia z opisanego w pkt 3a o przestrzeń urządzenia opisanego w pkt. 3b . Rozwiązanie musi pozwalać na przechowywanie min. 2 TB metadanych zdeduplikowanych danych w środowisku wirtualnym VMware pozwalając na przechowywanie kopii bezpieczeństwa na urządzeniu opisanym w pkt 3b z pominięciem urządzenia opisanego w pkt. 3a, które może pracować niezależnie. Licencje umożliwiające spełnienie ww. funkcjonalności muszą być dostarczone.
9. Zamawiający wymaga możliwości autonomicznej pracy urządzenia opisanego w pkt. 3a , a w razie potrzeby składowania kopii bezpieczeństwa na urządzeniu opisanym w pkt. 3b. Jednocześnie musi być spełniona funkcjonalność przechowywania min. 2 TB metadanych w środowisku wirtualnym VMware wraz ze składowaniem kopii bezpieczeństwa na urządzeniu opisanym w pkt 3b. Docelowym wymogiem Zamawiającego jest możliwość wykonywania kopii bezpieczeństwa systemów operacyjnych ze środowiska niezaufanego (notebooki, zdalne lokalizacje) przy wykorzystaniu urządzenia opisanego w pkt. 3a oraz wykonywanie kopii bezpieczeństwa ze środowiska zaufanego przy użyciu wirtualnego odpowiednika urządzenia opisanego w pkt 3a. Kopie bezpieczeństwa wykonywane z obu środowisk (zaufanego i niezaufanego) muszą mieć możliwość jednoczesnego składowania danych na urządzeniu opisanym w pkt 3b.
10. Rozwiązanie musi pozwalać na swobodne wykorzystanie przez Zamawiającego całej przestrzeni dyskowej pozostałej po zalicencjonowaniu zdeduplikowanych danych. System kopii bezpieczeństwa musi udostępniać przestrzeń dyskową protokołem NFS i CIFS.
11. Rozwiązanie musi być dostarczone z licencją wieczystą bez ograniczeń funkcjonalnych.
12. Zamawiający nie dopuszcza rozwiązania, w którym jakiekolwiek funkcjonalności dostarczanego rozwiązania będą niedostępne lub wyłączone, a ich uruchomienie będzie wymagało dokupienia dodatkowych licencji. Zamawiający nie wymaga dostarczenia licencji na replikację.
13. Rozwiązanie musi posiadać minimum 2 interfejsy 10 Gbps Ethernet RJ45 do przesyłania danych systemu kopii bezpieczeństwa z możliwością pracy w sieci 1Gbps Ethernet, minimum jeden interfejs zarządzający Ethernet oraz minimum 2 porty FC pozwalające na pracę w sieci SAN 8Gbps i 16 Gbps z możliwością obsługi przez każdy z portów sieci FC SAN. Rozwiązanie musi być podłączone do przełącznika Cisco Nexus 5596 – wymagane jest dostarczenie niezbędnego okablowania oraz modułów SFP do przełącznika.

14. Rozwiązanie musi być zainstalowane w szafach RACK 19”, a wszelkie okablowanie, szyny montażowe, przejściówki, konwertery, moduły, licencje oraz inne niewymienione, a niezbędne elementy do rozbudowy systemu kopii bezpieczeństwa w środowisku Zamawiającego muszą być dostarczone wraz z rozwiązaniem.
15. Rozwiązanie musi posiadać globalną dla całego rozwiązania deduplikację danych.
16. Dostarczone komponenty rozwiązania muszą być nowe, a termin End-Of-Support nie krótszy niż 5 lat od momentu dostarczenia rozwiązania.
17. Trwałe nośniki danych pozostają u Zamawiającego.
18. Rozwiązanie musi być firmowane przez jednego producenta systemu kopii bezpieczeństwa, poszczególne elementy systemu kopii bezpieczeństwa muszą być ze sobą zgodne technologicznie i znajdować się na liście zgodności oraz kompatybilności producenta, a wszelkie kontakty serwisowe muszą być obsługiwane przez jednego producenta.
19. Rozbudowa systemu kopii bezpieczeństwa nie może ograniczać obecnej funkcjonalności posiadanego systemu kopii bezpieczeństwa, a w szczególności: możliwości zabezpieczenia nieograniczonej liczby serwerów i komputerów fizycznych i wirtualnych, deduplikacji danych na źródle z blokami o zmiennej długości bez serwerów pośredniczących, możliwości zabezpieczania serwerów uruchomionych w klastrach hypervizorów VMware oraz Hyper-V, obsługi Change Block Tracking (CBT), integracji z Active Directory, możliwości kompresowania i szyfrowania przesyłanych danych kluczem kryptograficznym o długości min. 256 bitowym.
20. Rozwiązanie musi być dostarczone z minimum 5 letnim wsparciem producenta obejmującym: aktualizację systemu, naprawy w trybie NBD (następny dzień roboczy) u Zamawiającego, konsultacje techniczne.
21. Ilekroć Zamawiający stwierdza iż wymaga danej możliwości lub funkcjonalności, rozumie przez to dostarczenie takiej funkcjonalności bez jakichkolwiek dodatkowych opłat ze strony Zamawiającego. Niedopuszczalne jest dostarczenie rozwiązania w którym dana funkcjonalność możliwa jest do osiągnięcia po uiszczeniu ze strony Zamawiającego dodatkowych opłat – chyba, że Zamawiający wyraźnie to stwierdza.
22. W wyniku rozbudowy, system kopii bezpieczeństwa musi spełniać następujące funkcjonalności:

a) Fizyczny appliance opisany w pkt. 3a musi mieć następujące funkcjonalności:

1. Możliwość autonomicznej pracy – wykonywania kopii bezpieczeństwa i przechowywania ich na własnych, wewnętrznych dyskach
2. Możliwość przechowywania danych kopii bezpieczeństwa na urządzeniu opisanym w pkt. 3b
3. Wykonywanie kopii bezpieczeństwa lokalnego środowiska serwerowego, zdalnych lokalizacji serwerowych i zdalnych notebooków.
4. Zapis i przechowywanie kopii bezpieczeństwa na własnych dyskach powinien być realizowany bezpośrednio z wykorzystaniem deduplikacji

danych na źródle z blokami o zmiennej długości bez serwerów pośredniczących

5. Możliwość uruchomienia w przyszłości replikacji kopii bezpieczeństwa do zdalnego i zgodnego technologicznie urządzenia kopii bezpieczeństwa. Licencje do replikacji nie są wymagane.
6. Możliwość uruchomienia w przyszłości odtworzenia zreplikowanych kopii bezpieczeństwa ze zdalnego urządzenia. Licencje do replikacji nie są wymagane.
7. Urządzenie musi stanowić kompletny system wykonywania kopii bezpieczeństwa z agentami do serwerów fizycznych oraz bezagentowo systemów operacyjnych w środowiskach VMware i HyperV.
8. Obsługiwać wykonywanie i odtwarzanie kopii bezpieczeństwa serwerów fizycznych i wirtualnych systemów operacyjnych (UNIX/Linux/Windows) działających w zdalnych oddziałach oraz laptopów połączonych z centralą poprzez sieć WAN opartą o sieć telefonii komórkowej.
9. Tworzyć autonomiczny, centralny system kopii bezpieczeństwa zapewniający przechowywanie wszystkich zdeduplikowanych kopii zapasowych na własnych dyskach lub na dyskach oferowanego w pkt. 3b urządzenia.
10. Wykonywanie kopii bezpieczeństwa lokalnego środowiska serwerowego oraz zdalnych lokalizacji łączących się wolnymi łączami telekomunikacyjnymi np. technologią DSL, HSPA.
11. Zapis i przechowywanie zdeduplikowanych kopii bezpieczeństwa o pojemności min. 10 TB deduplikatów na dyskach dodatkowego urządzenia opisanego w pkt. 3b, zapis na zewnętrzne urządzenie musi być realizowany bez pośrednictwa dodatkowych serwerów.
12. Możliwość przeniesienia licencji pozwalającej na przechowywanie min. 5 TB deduplikatów na własnych dyskach do rozwiązania opisanego w pkt 3b umożliwiając przechowywanie min. 15 TB deduplikatów kopii bezpieczeństwa na urządzeniu opisanym w pkt 3b. Musi być możliwość wyboru liczby licencji do przeniesienia w zakresie od 1 do 5 TB.
13. W przyszłości replikację kopii bezpieczeństwa do zdalnego urządzenia. Dostarczenie licencji nie jest wymagane.
14. W przyszłości odtworzenie zreplikowanych kopii bezpieczeństwa ze zdalnego urządzenia. Dostarczenie licencji nie jest wymagane.
15. System musi przechowywać kopie bezpieczeństwa na własnych dyskach wewnętrznych appliance'u fizycznego.
16. Zainstalowane w urządzeniu oprogramowanie kopii bezpieczeństwa musi być dostarczone z licencją na nielimitowaną liczbę zabezpieczanych serwerów, procesorów, systemów operacyjnych, baz danych, datastore VMware, datastore HyperV oraz notebooków.
17. Rozwiązanie musi umożliwiać kopie bezpieczeństwa maszyn wirtualnych w trybie:
    1. obrazy maszyn wirtualnych z poziomu hipervizora VMware (vmdk), Hyper-V (vhd, vhdx),
    2. z wewnątrz systemu operacyjnego agentem plikowym
    3. z wewnątrz systemu operacyjnego agentem bazodanowym
    4. z wewnątrz agentem aplikacyjnym dla systemów plików Oracle, MS SQL, Exchange, Sharepoint
18. Oprogramowanie musi wspierać następujące systemy operacyjne: Windows (także Microsoft Cluster, Clustered Shared Volume) , Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu), Mac OS X, FreeBSD w wersjach aktualnych. A w trakcie wsparcia serwisowego uaktualnianie obsługi systemów operacyjnych o nowe wersje.
19. Kopie bezpieczeństwa zasobów z powyższych systemów operacyjnych muszą podlegać deduplikacji na źródle, tj. na zabezpieczanym

systemie operacyjnym.

20. Oprogramowanie kopii bezpieczeństwa musi wspierać kopie bezpieczeństwa online następujących baz danych i aplikacji: MS Exchange, MS SQL, Oracle, SharePoint, VMware, Hyper-V (w tym Hyper-V CSV). Kopie bezpieczeństwa z powyższych baz danych i aplikacji muszą podlegać deduplikacji na źródle, tj. na zabezpieczanym systemie operacyjnym.
21. Musi istnieć możliwość pobierania kopii zapasowej kilkoma strumieniami jednocześnie.
22. W przypadku zabezpieczania systemu Microsoft Exchange musi istnieć możliwość wykonania kopii bezpieczeństwa całego obrazu bazy danych i jednocześnie odtworzenia pojedynczego elementu bez konieczności odtwarzania całej bazy danych tzw. odtwarzanie granularne.
23. W przypadku zabezpieczania systemu Microsoft Sharepoint musi istnieć opcjonalna możliwość odtworzenia pojedynczego elementu systemu Sharepoint bez konieczności odtwarzania całego środowiska SharePoint, tzw. odtwarzanie granularne. Licencja na obsługę kopii bezpieczeństwa Microsoft SharePoint nie jest wymagana.
24. Oferowane rozwiązanie musi zabezpieczać zdeduplikowane dane Windows 2012 bez konieczności przywracania danych Windows 2012 do postaci oryginalnej, nie zdeduplikowanej.
25. Zabezpieczane serwery muszą być zabezpieczane bezpośrednio na medium urządzenia wykonującego kopie zapasowe (dyski appliance'u opisanego w pkt. 3a lub dyski oferowanego urządzenia przechowującego kopie zapasowe opisanego w pkt. 3b) bez pośrednictwa jakichkolwiek innych urządzeń lub serwerów. Funkcjonalność ta dotyczy zarówno kopii bezpieczeństwa lokalnych, zdalnych jak również kopii bezpieczeństwa notebooków.
26. Transfer danych z zabezpieczanych serwerów do oferowanego appliance'u (fizycznego i wirtualnego) nie może się odbywać po sieci SAN.
27. Oprogramowanie kopii bezpieczeństwa musi umożliwiać dla sieci lokalnej:
    1. kopie bezpieczeństwa pojedynczych plików
    2. kopie bezpieczeństwa całych systemów plików
    3. kopie bezpieczeństwa Bare Metal Recovery
    4. kopie bezpieczeństwa baz danych w trakcie ich normalnej pracy
    5. kopie bezpieczeństwa ustawień systemu operacyjnego Windows.
    6. kopie bezpieczeństwa całych obrazów maszyn wirtualnych systemu VMware (klaster)
    7. kopie bezpieczeństwa całych obrazów maszyn wirtualnych systemu Hyper-V (klaster)
28. Rozwiązanie kopii bezpieczeństwa musi transferować dane bezpośrednio ze zdalnych lokalizacji do appliance'u bez konieczności instalacji jakiegokolwiek sprzętu w zdalnej lokalizacji. Kopie bezpieczeństwa zdalnych lokalizacji muszą działać poprawnie nawet w przypadku wystąpienia opóźnień w sieci WAN przy jednoczesnej utracie pakietów.
29. Rozwiązanie kopii bezpieczeństwa nie może angażować personelu w zdalnej lokalizacji. Rozwiązanie kopii bezpieczeństwa musi działać w pełni funkcjonalnie przy założeniu, że pracownicy zdalnej lokalizacji nie angażują się w czynności wykonywania kopii bezpieczeństwa.
30. Rozwiązanie kopii bezpieczeństwa musi być w pełni konfigurowalne z konsoli znajdującej się w centralnej lokalizacji bez konieczności logowania się na zabezpieczany system operacyjny
31. Rozwiązanie kopii bezpieczeństwa musi mieć możliwość odtworzenia danych na docelowy system operacyjny w zdalnej lokalizacji z poziomu

centralnej konsoli systemu kopii bezpieczeństwa. Nie może być wymagane logowanie się na odtwarzany system operacyjny celem odtworzenia danych.

32. W przypadku odtwarzania całego systemu plików (partycja w Windows, system plików w Linux) rozwiązanie kopii bezpieczeństwa musi automatycznie porównać pliki znajdujące się w kopii bezpieczeństwa i pliki znajdujące się na odtwarzanym systemie operacyjnym, a następnie odtworzyć tylko brakujące dane, bez konieczności przesyłania pełnej kopii bezpieczeństwa. Powyższa funkcjonalność musi być spełniona również dla VMware CBT i Hyper-V RCT.
33. W celu minimalizacji ilości przesyłanych danych, oferowane rozwiązanie musi mieć możliwość przesyłania odtwarzanych danych z systemu kopii bezpieczeństwa do docelowego systemu operacyjnego w postaci skompresowanej, tak by odtwarzane dane były rozkompresowane na docelowym systemie operacyjnym przez agenta oferowanego systemu kopii bezpieczeństwa.
34. Rozwiązanie kopii bezpieczeństwa musi mieć funkcjonalność deduplikacji realizowaną poprzez podział danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki. Podział na bloki musi następować bezpośrednio na zabezpieczanym systemie operacyjnym na bloki o zmiennej długości.
35. Rozwiązanie kopii bezpieczeństwa musi zabezpieczać tylko unikalne bloki nie znajdujące się na docelowym systemie operacyjnym, skracając czas zabezpieczania danych, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.
36. Funkcjonalność deduplikacji danych nie może wymagać instalacji dodatkowych modułów programowych lub sprzętowych po stronie klienckiej
37. Rozwiązanie kopii bezpieczeństwa musi wykonywać zawsze wyłącznie pełne kopie bezpieczeństwa danych. Do appliance'u muszą być wysyłane dane po deduplikacji, natomiast sama kopia bezpieczeństwa danych musi być logicznie pełną kopią bezpieczeństwa.
38. W rozwiązaniu kopii bezpieczeństwa musi być możliwość definiowania czasu ważności zabezpieczanych danych na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności kopie bezpieczeństwa muszą być automatycznie usunięte.
39. Oferowanie rozwiązanie kopii bezpieczeństwa musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu GFS (Dziadek–ojciec–syn), to znaczy utworzenia polityki w której zdefiniowano:
    1. czas przechowywania kopii bezpieczeństwa dziennych
    2. czas przechowywania kopii bezpieczeństwa tygodniowych
    3. czas przechowywania kopii bezpieczeństwa miesięcznych
    4. czas przechowywania kopii bezpieczeństwa rocznych
40. Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających kopii bezpieczeństwa w ramach zadania zabezpieczającego dane. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:
    1. wybranych typów plików, np. na podstawie rozszerzenia
    2. dla katalogów (np.: c:\windows).
    3. dla partycji np. C:\
    4. dla pojedynczych plików
    5. dla dysków wirtualnych np. vmdk, vhdx

41. Oferowane rozwiązanie musi mieć możliwość zdefiniowania aby ostatnia kopia bezpieczeństwa zabezpieczanych danych nigdy się nie przeterminowała. Oznacza to, że jeśli dany zasób nie jest zabezpieczany to automatycznie ostatnia kopia bezpieczeństwa tego zasobu jest przechowywana bezterminowo i jedynie administrator systemu kopii bezpieczeństwa może zdecydować o jego usunięciu.
42. Niezależnie od dostarczonego urządzenia (appliance fizyczny) musi istnieć możliwość zainstalowania analogicznego serwera (appliance'u wirtualnego) kopii bezpieczeństwa na platformie hypervizora:
    1. VMware ESX (appliance wirtualny)
    2. Hyper-V (appliance wirtualny)

    o tej samej funkcjonalności oraz pojemności przechowywania w środowisku wirtualnym takiej ilości metadanych przy której producent rozwiązania zagwarantuje techniczną możliwość wykorzystania pełnej pojemności użytkowej urządzenia opisanego w pkt 3b. Musi istnieć możliwość swobodnej migracji licencji z urządzenia opisanego w pkt. 3a do wirtualnego appliance'u, uzyskując na wirtualnym appliance możliwość przechowywania min. 15 TB zdeduplikowanych danych na urządzeniu opisanym w pkt. 3b. Pozostała przestrzeń urządzenia opisanego w pkt. 3b musi być możliwa do wykorzystania przez Zamawiającego protokołem CIFS lub NFS.
43. Oferowane rozwiązanie musi mieć możliwość replikacji danych z przyszłościowym appliancem wirtualnym w obu kierunkach jednocześnie:
    1. appliance fizyczny w ośrodku A do appliance wirtualny w ośrodku B
    2. appliance wirtualny w ośrodku B do appliance fizyczny w ośrodku A
    3. appliance wirtualny w ośrodku A do appliance wirtualny w ośrodku B
44. Replikacji muszą podlegać tylko zmienione bloki. Musi istnieć możliwość zdefiniowania kalendarza replikacji między appliance'mi. Licencja na replikację nie jest wymagana.
45. Konsola zarządzająca systemem kopii zapasowych musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory ról u uprawnień występujących w systemie kopii bezpieczeństwa (m.in. pełna kontrola, tylko do odczytu, tylko wykonywanie odtworzeni zabezpieczanych danych). Musi być możliwość przedzielania uprawnień do poszczególnych zadań kopii bezpieczeństwa
46. Konsola systemu kopii bezpieczeństwa musi udostępniać raporty dotyczące zajętości przestrzeni przez zabezpieczane dane w tym zajętość przestrzeni przeznaczonej na dane zdeduplikowane.
47. Konsola systemu kopii bezpieczeństwa musi powiadamiać o błędach, awariach, niewykonaniu kopii bezpieczeństwa, kończącym się miejscu, wygasającym wsparciu w postaci: e-mail, SNMP i komunikatów w konsoli
48. Bloki przesyłane z zabezpieczanych systemów operacyjnych do appliance'a lub do oferowanego urządzenia opisanego w pkt. 3b muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256 bitowym.
49. Wymagana możliwość szyfrowania danych na medium przechowującym zabezpieczane dane. Licencja szyfrowania musi być dostarczona w

ramach postępowania.

50. Wymagane uwierzytelnianie komunikacji między klientem, a systemem kopii bezpieczeństwa oparte na certyfikatach kryptograficznych
51. System kopii bezpieczeństwa musi pozwalać na odtwarzanie danych: całości zabezpieczanych danych, wybiórcze odtwarzanie zabezpieczanych danych, przy czym odtwarzanie musi być realizowane w jednym procesie tj. np. bez odtwarzania całości zabezpieczanych danych, a następnie wybranego pliku.
52. System kopii bezpieczeństwa musi mieć możliwość limitowania rozmiaru danych zadania. Jeśli zadanie przekroczy zdefiniowany rozmiar zabezpieczanych danych - wówczas nie może być zapisane w systemie kopii bezpieczeństwa
53. System kopii bezpieczeństwa musi mieć możliwość limitowania czasu trwania zadania. Jeśli zadanie przekroczy zdefiniowaną wartość czasową, wówczas nie może być zapisane w systemie kopii bezpieczeństwa
54. System kopii bezpieczeństwa musi wspierać wykonywanie kopii bezpieczeństwa i odtwarzanie kopii bezpieczeństwa zabezpieczanych danych serwerów wirtualnych pracujących w klastrowych środowiskach VMware ESX/vCenter 4.1/5.0/5.5/6.0/6.5.
55. System kopii bezpieczeństwa musi umożliwiać dla środowisk VMware następujące typy kopii bezpieczeństwa:
    a. Zabezpieczanie danych całych maszyn wirtualnych
    b. Zabezpieczanie pojedynczych, wybranych dysków maszyny wirtualnej vmdk
    c. Zabezpieczanie danych przy użyciu kryterium wyrażeń regularnych
    d. Odtwarzanie zabezpieczanych danych musi obsługiwać przesyłanie tylko zmienionych bloków serwerów wirtualnych VMWare (wymagane wykorzystanie mechanizmu CBT VMWare)
    e. Powyższe metody zabezpieczania danych maszyn wirtualnych muszą podlegać procesowi deduplikacji przed przesłaniem danych do medium przechowującego kopie bezpieczeństwa
    f. Powyższe metody zabezpieczania danych muszą być wbudowane w system kopii bezpieczeństwa i w pełni automatyczne bez ingerencji administratora systemu kopii bezpieczeństwa w skrypty czy dodatkowe komendy
56. System kopii bezpieczeństwa musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z oferowanego urządzenia przechowującego kopie bezpieczeństwa, bez konieczności odtwarzania kopii bezpieczeństwa. Uruchomiony serwer wirtualny musi być w pełni funkcjonalny w środowisku produkcyjnym Zamawiającego. Zamawiający nie wymaga identycznej z serwerem produkcyjnym wydajności serwera

wirtualnego uruchomionego bezpośrednio z kopii bezpieczeństwa.

57. System kopii bezpieczeństwa musi mieć możliwość przeglądania, bez konieczności odtwarzania zabezpieczanych danych, plików i katalogów zabezpieczanych danych. Funkcjonalnośc ta musi być dostępna dla wszystkich trybów kopii bezpieczeństwa: pełnych obrazów maszyn wirtualnych, plików vmdk, vhdx, pozwalając na ich przeszukiwanie (wymagane przeszukiwanie po nazwach plików)
58. System kopii bezpieczeństwa musi mieć możliwość tworzenia i odtworzenia kopii bezpieczeństwa w trybie „image backup” (backup plików vmdk) maszyn wirtualnych pracujących w środowisku klastrowym VMware ESX bez udziału vCenter.
59. Wymagana obsługa przez system kopii bezpieczeństwa dla środowisk VMware na poziomie minimum 1000 maszyn wirtualnych
60. System kopii bezpieczeństwa musi mieć możliwość automatycznej weryfikacji wykonanych kopii bezpieczeństwa maszyn wirtualnych VMware. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware.
61. Weryfikacja maszyn wirtualnych czyli tzw. testowanie kopii bezpieczeństwa musi zapewniać minimum:
    a. Odtworzenie maszyny wirtualnej na zdefiniowanym DataCenter oraz Datastore
    b. Weryfikację podstawowych procesów odtwarzanego serwera
    c. Informację w konsoli systemu kopii bezpieczeństwa o poprawnej lub niepoprawnej weryfikacji maszyny wirtualnej
62. Administrator danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego odtworzenia pojedynczych plików z dowolnej kopii bezpieczeństwa jego maszyny wirtualnej bez konieczności kontaktu z administratorem systemu kopii bezpieczeństwa czy też administratorem systemu VMware. Wymagana jest w tej funkcjonalności integracja z Active Directory.
63. System kopii bezpieczeństwa musi zawsze przechowywać pełne kopie bezpieczeństwa obrazów maszyn wirtualnych środowiska VMware dla każdej wykonanej w przeszłości kopii zapasowej. Każda kopia bezpieczeństwa obrazu maszyny wirtualnej musi być pełna kopią bezpieczeństwa.
64. System kopii bezpieczeństwa musi pozwalać na automatyczne polityki kopii bezpieczeństwa w środowisku Vmware dla:
    a. Folderu
    b. Resource Pool

    Dodanie lub usunięcie maszyny wirtualnej do/z folderu, hosta czy Resource Pool w systemie VMware spowoduje automatyczne dodanie lub usunięcie maszyny wirtualnej z polityki zdefiniowanej dla danego folderu, hosta ESX, klastra czy resource pool w systemie VMware.

65. System kopii bezpieczeństwa musi umożliwiać definiowanie polityk kopii bezpieczeństwa dostępnych dla administratora systemu VMware z poziomu VMware vCenter. Administrator VMware musi mieć możliwość przydzielania obecnych jak i nowo tworzonych maszyn wirtualnych do polityk kopii bezpieczeństwa
66. System kopii bezpieczeństwa musi automatycznie wykrywać i naprawiać problemy związane z migawkami (snapshotami) VMware. W przypadku gdy system VMware nie usunie migawki, system kopii bezpieczeństwa automatycznie ponowi usunięcie migawki, a w razie potrzeby wykona automatyczną konsolidację maszyny wirtualnej VMware.
67. Istnienie migawki maszyny wirtualnej nie może być przeszkodą w wykonaniu kopii bezpieczeństwa maszyny wirtualnej.
68. Kopie bezpieczeństwa maszyn wirtualnych oraz odtworzenie maszyn wirtualnych VMware musi być możliwe z poziomu graficznego interfejsu (GUI) oraz linii komend (CLI)
69. System kopii bezpieczeństwa musi umożliwiać dla środowisk Hyper-V oraz klastrowych środowiskach Microsoft Hyper-V 2012 R2 (CSV):
    a. Zabezpieczanie danych pojedynczych plików i baz danych z wewnątrz systemu operacyjnego uruchomionego w Hyper-V.
    b. Zabezpieczanie całych maszyn wirtualnych (w tym plików vhd, vhdx)
    c. Zabezpieczanie danych całych maszyn wirtualnych (w tym plików vhd, vhdx) musi pozwalać na odtworzenie pojedynczych plików lub folderów bez konieczności odtworzenia pełnej kopii bezpieczeństwa. Funkcjonalność musi dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows.
    d. Oprogramowanie musi wspierać technologię Microsoft RCT (Resilient Change Tracking). Dopuszcza się wykonywanie snapshotów VSS maszyn wirtualnych i użycie ich w trakcie backupu obrazów maszyn wirtualnych.
    e. Powyższe metody zabezpieczania danych maszyn wirtualnych muszą podlegać procesowi deduplikacji przed przesłaniem danych do medium przechowującego kopie bezpieczeństwa
    f. Powyższe metody zabezpieczania danych muszą być wbudowane w system kopii bezpieczeństwa i w pełni automatyczne bez ingerencji administratora systemu kopii bezpieczeństwa w skrypty czy dodatkowe komendy
70. System kopii bezpieczeństwa musi zapewniać zabezpieczanie danych Microsoft Exchange oraz MS SQL w przypadku zabezpieczania całych obrazów systemów operacyjnych uruchomionych w środowisku Hyper-V. Wymagane są następujące scenariusze odtwarzania danych:
    a. bezpośrednio z zabezpieczanego systemu operacyjnego

b. z konsoli systemu kopii bezpieczeństwa

c. możliwość odtworzenia pojedynczego lub folderu

d. możliwość odtworzenia zabezpieczanej bazy danych

71. Dla wspieranych systemów operacyjnych musi istnieć funkcjonalność odtwarzania danych w postaci Bare Metal Recovery tj. automatycznego i kompleksowego odtworzenia całego serwera (wszystkie partycje) w jednym kroku bezpośrednio z oferowanego rozwiązania. Funkcjonalność musi być wbudowana w rozwiązanie systemu kopii bezpieczeństwa.

72. W przypadku odtwarzania danych z interfejsu dostępnego na zabezpieczanym systemie operacyjnym, musi istnieć mechanizm uwierzytelniania użytkowników dostępny w dwóch wariantach:

    a. wbudowany w system backupowy (wewnętrzna baza użytkowników)

    b. zintegrowany z usługami katalogowymi Active Directory - użytkownicy będący w domenie nie muszą się logować do systemu backupu w przypadku konieczności odtworzenia danych, przeszukania zawartości kopii bezpieczeństwa oraz wykonania kopii bezpieczeństwa

73. Odtwarzanie danych z interfejsu końcowego użytkownika dostępnego na zabezpieczanym systemie operacyjnym musi umożliwiać wyszukiwanie plików np. po nazwie pliku itp.

74. System kopii bezpieczeństwa musi umożliwiać odtworzenie danych zlecając proces odtwarzania poprzez przeglądarkę internetową. Odtwarzanie to musi zapewniać uwierzytelnienie użytkownika oraz wyszukiwanie pliku lub folderu po nazwie.

75. W przypadku odtwarzania danych do systemu operacyjnego, który posiada dane, system kopii bezpieczeństwa musi automatycznie sprawdzać, których danych znajdujących się w kopii bezpieczeństwa brakuje na odtwarzanym systemie operacyjnym, a następnie przesyłać tylko te dane, których brakuje na odtwarzanym systemie operacyjnym.

76. System kopii bezpieczeństwa musi pracować z dostępnością w przypadku operacji wykonywania i odtwarzania kopii bezpieczeństwa przez 24h na dobę, 7 dni w tygodniu - w standardowym cyklu pracy. Wewnętrzne operacje maintenance'owe systemu kopii bezpieczeństwa np. sprawdzanie błędów, deduplikacja, oczyszczanie systemu ze starych kopii bezpieczeństwa itp. nie mogą uniemożliwiać procesu wykonywania kopii bezpieczeństwa czy odtwarzania danych w trakcie takiego procesu. Dopuszczalne jest jedynie spowolnienie procesu wykonywania lub odtwarzania kopii bezpieczeństwa.

77. System kopii bezpieczeństwa musi mieć możliwość raportowania błędów bezpośrednio do serwisu producenta. Funkcjonalność taka musi

mieć możliwość wyłączenia takiego raportowania.

78. System kopii bezpieczeństwa musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji wdrażania agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanym systemie operacyjnym
79. System kopii bezpieczeństwa musi mieć możliwość automatycznej aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta. Instalacja taka musi być zatwierdzona przez administratora.
80. System kopii bezpieczeństwa musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z systemu kopii bezpieczeństwa
81. Wymagane wsparcie realizowane przez producenta do maksymalnego terminu jakie producent może zagwarantować na posiadane urządzenie (end-of-support) licząc od dnia końca gwarancji określonej w pkt. 2, w trybie NBD (Następny dzień roboczy) w cyklu 5 dni w tygodniu w obrębie oprogramowania i sprzętu systemu kopii bezpieczeństwa, gwarantujące dostęp do: najnowszych wersji oprogramowania, aktualizacji, poprawek i upgrade'u systemu i aplikacji, konsultacji telefonicznych w języku polskim, wsparcia serwisowego oraz gwarancyjnego.
82. Wymagana polska wersja językowa interfejsu użytkownika końcowego dostępnego na zabezpieczanym systemie operacyjnym, dedykowanego do odtwarzania danych przez użytkownika końcowego.
83. Możliwość odtwarzania Active Directory z kopii bezpieczeństwa
84. Możliwość wykonywania o odtwarzania kopii bezpieczeństwa w środowisku klastrowym MS SQL oraz Oracle
85. Wsparcie do zabezpieczania i odtwarzania danych w systemie operacyjnym: Wsparcie systemów operacyjnych:
    a. Windows Server 2003/2003R2/2008/2008R2/2012/2012R2/2016 with Hyper-V
    b. Windows Vista/7/8.1/8/10
    c. Linux (CentOS 5/6/7, Ubuntu 12/14/16, Debian 7/8/9
    d. VMware ESX 4.1/5.0/5.5/6.0/6.5 (bezagentowo)
86. Bezagentowe wykonywanie kopii bezpieczeństwa z hypervizorów VMware oraz Hyper-V ze wsparciem technologii VMware Change Block Tracking (CBT) i Hyper-V Resilient Change Tracking (RCT)

87. Wsparcie systemu kopii bezpieczeństwa dla dysków dynamicznych oraz dysków partycjonowanych zgodnie z GPT
88. System kopii zapasowych musi mieć możliwość ustawienia rotacji kopii bezpieczeństwa oraz zdefiniowania polityk retencji.

b) Fizyczne urządzenie do składowania danych kopii bezpieczeństwa opisane w pkt. 3b musi mieć następujące funkcjonalności:

1. Użyteczną przestrzeń dyskową o pojemności min. 70 TB (+/- 1 TB).
2. Urządzenie musi być dedykowane i w pełni kompatybilne do pracy z urządzeniem opisanym w pkt. 3a
3. Możliwość przechowywania danych o łącznej pojemności min. 10 TB zdeduplikowanych danych z urządzenia opisanego w pkt. 3a, a w przypadku migracji licencji z urządzenia opisanego w pkt. 3a do wirtualnego apllicance'u – możliwość przechowywania min. 15 TB zdeduplikowanych danych.
4. Rozbudowa do większej pojemności powinna być możliwa poprzez bezpośrednie dołożenie kolejnych półek z dyskami oraz odpowiednich licencji, rozbudowa nie może być realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń.
5. Funkcjonalność deduplikacji danych w czasie rzeczywistym (tzw. „w locie") i być dedykowane do przechowywania kopii zapasowych przez producenta systemu kopii zapasowych.
6. Rozwiązanie opisane w pkt 3b musi być skalowalne do przestrzeni użytkowej minimum 150 TB (+/- 10 TB) w ramach tego samego urządzenia, rozbudowa do wymaganej pojemności musi być możliwa poprzez dołożenie kolejnych dysków lub kolejnych półek z dyskami oraz odpowiednich licencji, rozbudowa nie może być realizowana poprzez zwielokrotnienie ilości oferowanych urządzeń.
7. Rozwiązanie musi posiadać minimum 2 interfejsy 10 Gbps Ethernet RJ45 do przesyłania danych systemu kopii bezpieczeństwa z możliwością pracy w sieci 1Gbps Ethernet, minimum jeden interfejs zarządzający Ethernet oraz minimum 2 porty FC pozwalające na pracę w sieci SAN 8Gbps i 16 Gbps z możliwością obsługi przez każdy z portów sieci FC SAN. Rozwiązanie musi być podłączone do przełącznika Cisco Nexus 5596 – wymagane jest dostarczenie niezbędnego okablowania oraz modułów SFP do przełącznika.
8. Pozwalać na jednoczesny dostęp protokołami CIFS i NFS dla Ethernet oraz jednocześnie FC SAN w obrębie oferowanej pojemności urządzenia
9. Funkcjonalność szyfrowania przechowywanych danych w obrębie całej, zamawianej pojemności urządzenia
10. Wszystkie zapisywane strumienie danych muszą podlegać globalnej deduplikacji realizowanej w czasie rzeczywistym (deduplikacja „w locie",

in-line)

11. Funkcjonalność deduplikacji musi wykorzystywać algorytm bazujący na zmiennym bloku.
12. Globalna deduplikacja dla danych przesyłanych jednocześnie protokołami (CIFS, NFS, SAN)
13. Kompresja przechowywanych danych
14. Przy przesyłaniu danych interfejsem Ethernet, musi być możliwość szyfrowania komunikacji kluczem minimum AES 256 bitów
15. Urządzenie powinno dopuszczać wykorzystanie powierzchni użytecznej do 90% jej powierzchni. Dokumentacja urządzenia nie może wskazywać na jakiekolwiek problemy czy obostrzenia, które mogą pojawić się przy zapełnieniu urządzenia do 90% powierzchni użytecznej.
16. Umożliwiać bezpośrednią replikację danych (bez pośrednictwa dodatkowych urządzeń) do drugiego urządzenia tego samego lub podobnego typu. Replikacja musi się odbywać co najmniej w trybie asynchronicznym. Transmitowane muszą być tylko zmienione dane. Ewentualna licencja na replikację nie musi być dostarczona w ramach postępowania.
17. Urządzenie musi umożliwiać wydzielenie określonych interfejsów sieciowych do mechanizmów replikacji danych
18. Możliwość ograniczenia pasma używanego do replikacji danych między dwoma urządzeniami, przy pomocy wbudowanych funkcjonalności lub harmonogramu replikacji danych
19. Dane przechowywane w systemie kopii bezpieczeństwa (w tym dane zdeduplikowane i skompresowane) muszą być chronione za pomocą technologii RAID pozwalającej na awarie min. 2 dysków twardych w obrębie jednej grupy RAID
20. Dyski twarde muszą obsługiwać technologię hot-swap, czyli wyjmowanie i wkładanie dysków twardych w trakcie pracy urządzenia
21. Oferowane urządzenie musi umożliwiać wykonywanie i odtwarzanie migawek (snapshotów) przechowywanych danych
22. Odtworzenie danych z migawki nie może wymagać konieczności nadpisania danych produkcyjnych ani przerwy w normalnej pracy urządzenia
23. Urządzenie musi pozwalać na podział na logiczne części
24. Dla każdej z logicznych części oferowanego urządzenia musi być możliwość separacji uprawnień dostępu do przechowywanych danych w postaci zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią urządzenia przechowującego dane.
25. Wymagana możliwość obsługi każdej z logicznych części oferowanego urządzenia protokołami CIFS i NFS

26. Urządzenie musi automatycznie usuwać przeterminowane dane w procesie wewnętrznego oczyszczania, przy czym proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy urządzenia w pełnej funkcjonalności.
27. Urządzenie musi mieć możliwość zarządzania poprzez: interfejs graficzny (GUI) dostępny z przeglądarki internetowej oraz poprzez linię komend (CLI) dostępną poprzez SSH (secure shell). Oprogramowanie do zarządzania musi być dostarczone wraz z oferowanym urządzeniem
28. Oferowane urządzenie musi mieć możliwość weryfikacji pakietu firmware urządzenia chroniącego przed aktualizacją do błędnej wersji oprogramowania i sprawdzającego czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
29. Urządzenie musi być rozwiązaniem kompletnym, pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway, serwer pośredniczący. Urządzenie musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postepowania.
30. Wymagane wsparcie realizowane przez producenta przez okres min. 5 lat w trybie NBD (Następny dzień roboczy) w cyklu 5 dni w tygodniu w obrębie oprogramowania i sprzętu systemu kopii bezpieczeństwa, gwarantujące dostęp do: najnowszych wersji oprogramowania, aktualizacji, poprawek i upgrade'u systemu i aplikacji, konsultacji telefonicznych w języku polskim, wsparcia serwisowego oraz gwarancyjnego.
31. Możliwość uwierzytelnienia użytkowników poprzez usługę katalogową np. Active Directory

c) Licencje określone w pkt 3c muszą się spełniać następujące wymogi:

1. Nie mogą charakteryzować się ograniczeniami czasowymi ani funkcjonalnymi.
2. Musi być możliwość swobodnej migracji przez Zamawiającego licencji między appliance'ami dostosowując ich rozkład do bieżących potrzeb Zamawiającego oraz składowania tych danych na urządzeniu opisanym w pkt 3b.
3. Licencje muszą być zarejestrowane na dane Zamawiającego.
4. Zamawiający wymaga możliwości autonomicznej pracy urządzenia opisanego w pkt. 3a , a w razie potrzeby składowania danych na urządzeniu opisanym w pkt. 3b. Jednocześnie musi być spełniona funkcjonalność przechowywania w środowisku wirtualnym VMware takiej ilości metadanych przy której producent rozwiązania zagwarantuje techniczną możliwość wykorzystania pełnej pojemności użytkowej urządzenia opisanego w pkt 3b.
5. Docelowym wymogiem Zamawiającego jest możliwość wykonywania kopii bezpieczeństwa systemów operacyjnych ze środowiska

niezaufanego (notebooki, zdalne lokalizacje) przy wykorzystaniu urządzenia opisanego w pkt. 3a, a wykonywanie kopii bezpieczeństwa ze środowiska zaufanego przy użyciu wirtualnego odpowiednika urządzenia opisanego w pkt. 3a. Kopie bezpieczeństwa wykonywane z obu środowisk (zaufanego i niezaufanego) muszą mieć możliwość jednoczesnego składowania danych na urządzeniu opisanym w pkt 3b.

6. Dostarczone rozwiązanie musi pozwalać na migrację licencji z urządzenia opisanego w pkt. 3a do rozwiązania będącego wirtualnym odpowiednikiem urządzenia opisanego w pkt. 3a. umożliwiając zsumowanie liczby licencji na przechowywanie deduplikatów kopii bezpieczeństwa na urządzeniu opisanym w pkt 3b.
7. Wymagane wsparcie realizowane przez producenta przez okres min. 5 lat w trybie NBD (Następny dzień roboczy) w cyklu 5 dni w tygodniu w obrębie oprogramowania systemu kopii bezpieczeństwa, gwarantujące dostęp do: najnowszych wersji oprogramowania, aktualizacji, poprawek i upgrade'u systemu i aplikacji, konsultacji telefonicznych w języku polskim, wsparcia serwisowego oraz gwarancyjnego.

d) Całość systemu kopii bezpieczeństwa musi spełniać następujące wymogi:

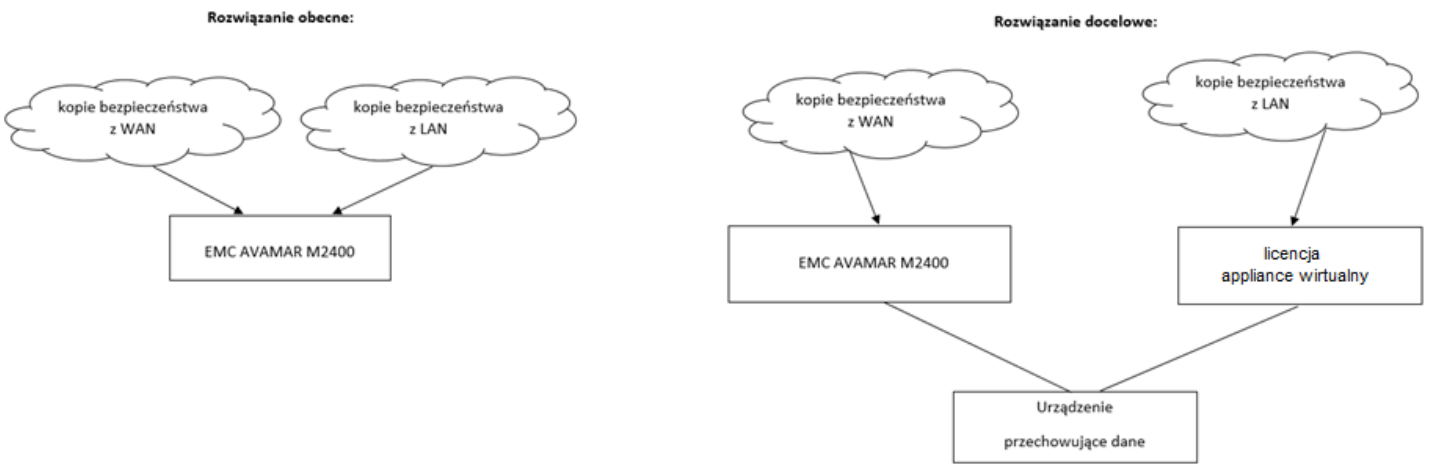
1. System kopii bezpieczeństwa musi obsługiwać systemy operacyjne (UNIX/Linux/Windows), działające zarówno na serwerach fizycznych jak i wirtualnych
2. System musi tworzyć centralny system kopii bezpieczeństwa oraz zapewniać przechowywanie wszystkich zdeduplikowanych danych na dyskach twardych urządzeń będących integralną częścią systemu kopii bezpieczeństwa.
3. Rozwiązanie musi być firmowane przez jednego producenta systemu kopii bezpieczeństwa, poszczególne elementy systemu kopii bezpieczeństwa muszą być ze sobą zgodne technologicznie i znajdować się na liście zgodności oraz kompatybilności producenta, a wszelkie kontakty serwisowe muszą być obsługiwane przez jednego producenta.
4. Rozwiązanie musi być dostarczone z licencją wieczystą bez ograniczeń funkcjonalnych.
5. Trwałe nośniki danych pozostają u Zamawiającego.
6. System kopii bezpieczeństwa musi się charakteryzować w szczególności funkcjonalnościami: możliwość zabezpieczenia nieograniczonej liczby serwerów i komputerów fizycznych i wirtualnych, deduplikacji danych na źródle z blokami o zmiennej długości bez serwerów pośredniczących, możliwości zabezpieczania serwerów uruchomionych w klastrach hypervizorów VMware oraz Hyper-V, obsługi Change Block Tracking (CBT), integracji z Active Directory, możliwości kompresowania i szyfrowania przesyłanych danych kluczem kryptograficznym o długości min. 256 bitowym.
7. Zamawiający nie dopuszcza rozwiązania, w którym jakiekolwiek funkcjonalności dostarczanego rozwiązania będą niedostępne lub wyłączone, a

ich uruchomienie będzie wymagało dokupienia dodatkowych licencji. Zamawiający nie wymaga dostarczenia licencji na replikację.

8. Rozwiązanie musi posiadać minimum 2 interfejsy 10 Gbps Ethernet RJ45 do przesyłania danych systemu kopii bezpieczeństwa z możliwością pracy w sieci 1Gbps Ethernet, minimum jeden interfejs zarządzający Ethernet oraz minimum 2 porty FC pozwalające na pracę w sieci SAN 8Gbps i 16 Gbps z możliwością obsługi przez każdy z portów sieci FC SAN. Rozwiązanie musi być podłączone do przełącznika Cisco Nexus 5596 – wymagane jest dostarczenie niezbędnego okablowania oraz modułów SFP do przełącznika.
9. Rozwiązanie musi być zainstalowane w szafach RACK 19”, a wszelkie okablowanie, szyny montażowe, przejściówki, konwertery, moduły, licencje oraz inne niewymienione, a niezbędne elementy do rozbudowy systemu kopii bezpieczeństwa w środowisku Zamawiającego muszą być dostarczone wraz z rozwiązaniem.
10. Dostarczone komponenty rozwiązania muszą być nowe, a termin End-Of-Support nie krótszy niż 5 lat od momentu dostarczenia rozwiązania
11. Wymagane wsparcie realizowane przez producenta przez okres min. 5 lat w trybie NBD (Następny dzień roboczy) w cyklu 5 dni w tygodniu w obrębie dostarczonego oprogramowania i sprzętu systemu kopii bezpieczeństwa, gwarantujące dostęp do: najnowszych wersji oprogramowania, aktualizacji, poprawek i upgrade’u systemu i aplikacji, konsultacji telefonicznych w języku polskim, wsparcia serwisowego oraz gwarancyjnego.
12. Ilekroć Zamawiający stwierdza iż wymaga danej możliwości lub funkcjonalności, rozumie przez to dostarczenie takiej funkcjonalności bez jakichkolwiek dodatkowych opłat ze strony Zamawiającego. Niedopuszczalne jest dostarczenie rozwiązania w którym dana funkcjonalność możliwa jest do osiągnięcia po uiszczeniu ze strony Zamawiającego dodatkowych opłat – chyba, że Zamawiający wyraźnie to stwierdza.

e) Schemat poglądowy rozbudowy systemu kopii bezpieczeństwa przedstawiono na Rysunku 1.

Schemat poglądowy:



Rysunek 1. Schemat poglądowy rozbudowy systemu kopii bezpieczeństwa