EZP.26.58.10.2024.JK Warszawa, dnia 18.07.2024 r.

Dotyczy postępowania o udzielenie zamówienia publicznego pn. **Zakup subskrypcji systemu kopii zapasowej wraz z wdrożeniem i wsparciem technicznym,** *oznaczenie sprawy:* EZP.26.58.2024

WYJAŚNIENIE i ZMIANA TREŚCI SPECYFIKACJI WARUNKÓW ZAMÓWIENIA (SWZ)

I. Zamawiający działając na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych (t.j. Dz. U. 2023, poz. 1605 z późn. zm.), zwanej dalej „Ustawą Pzp" informuje o zmianie treści SWZ w związku z wniesieniem do Prezesa Krajowej Izby Odwoławczej odwołania na zapisy Specyfikacji Warunków Zamówienia.

Zamawiający dokonuje zmiany treści załącznika nr 1 do SWZ – Opis przedmiotu zamówienia.

Aktualna treść ww. załącznika stanowi załącznik do niniejszego pisma.

II. Zamawiający działając na podstawie art. 284 ust. 1 ustawy Prawo zamówień publicznych (t.j. Dz. U. 2023, poz. 1605, ze zm.), zwanej dalej „Ustawą Pzp" informuje, iż w ww. postępowaniu wpłynęły zapytania do treści SWZ.

W związku z powyższym na podstawie art. 284 ust. 6 i ust. 3 oraz art. 286 ust 1 Ustawy Pzp, Zamawiający wyjaśnia i zmienia treść Specyfikacji Warunków Zamówienia.

W przypadku, gdy udzielone poniżej odpowiedzi pozostają w sprzeczności z postanowieniami SWZ lub też precyzują lub uzupełniają postanowienia SWZ, należy przyjąć, że stanowią one zmianę SWZ, dokonaną przez Zamawiającego w myśl art. 286 ust. 1 Ustawy Pzp i będą stanowić podstawę dla oceny zgodności oferty z SWZ, przy czym w przypadku gdy:

1. postanowienia odpowiedzi są sprzeczne z postanowieniami SWZ, za obowiązujące w tym zakresie należy przyjąć treść udzielonej odpowiedzi,
2. postanowienia odpowiedzi precyzują lub uzupełniają postanowienia SWZ, za obowiązujące w tym zakresie należy przyjąć treść udzielonych odpowiedzi wraz z dotychczasową treścią SWZ.

Pytanie 1:

Czy zamawiający dopuszcza instalację serwera zarządzającego jako maszyny wirtualnej w obu lokalizacjach? – skonfigurowana funkcja replikacji konfiguracji w celu zapewnienia wysokiej dostępności.

Odpowiedź:

Zamawiający informuje, iż dopuszcza instalację serwera zarządzającego jako maszyny wirtualnej w obu lokalizacjach.

Pytanie 2:

Czy zamawiający dopuszcza doposażenie przez wykonawcę serwerów backupu w karty NVME?

Odpowiedź:

Zamawiający informuje, iż dopuszcza doposażenie przez Wykonawcę serwerów backupu w karty NVME pod warunkiem, że będą one kompatybilne z posiadanymi przez Zamawiającego serwerami.

Pytanie 3:

Ile dostępnej przestrzeni (nie zaalokowanej) przestrzeni jest na macierzach IBM?

Odpowiedź:

Zamawiający informuje, iż przestrzeń na macierzach IBM jest zaalokowana w 100%

Pytanie 4:

W jakiej lokalizacji umieszczona jest macierz QSAN?

Odpowiedź:

Zamawiający informuje, iż lokalizacja serwerowni głównej w Warszawie, przy ul. Jagiellońskiej 76.

Pytanie 5:

W jakie dyski (SSD / NLSAS) wyposażona jest macierz QSAN?

Odpowiedź:

Zamawiający informuje, iż Macierz QSAN zawiera trzy rodzaje modeli dysków: HUSMM1620ASS200, HUC101860CSS200, SDLL1DLR400GCCA1.

ul. Rakowiecka 4, 00-975 Warszawa
tel. (+48) 22 45 92 000, biuro@pgi.gov.pl

Sąd Rejonowy dla m. st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS, Nr 0000122099
NIP 525-000-80-40

Pytanie 6:

Jaka jest retencja backupów w TSM?

Odpowiedź:

Zamawiający informuje, iż dokładne informacje na temat retencji backupów zostaną przekazane Wykonawcy po zawarciu umowy

Pytanie 7:

Czy wszystkie backupowane dane mieszczą się na dyskach czy cześć backupów wykonywana jest bezpośrednio na taśmę?

Odpowiedź:

Zamawiający informuje, iż backupy wykonywane są bezpośrednio na dyski. Na taśmy trafiają poprzednie kopie backupów.

Pytanie 8:

Czy będzie możliwe stworzenie nowej partycji na bibliotece taśmowej na potrzeby nowego systemu backupu?

Odpowiedź:

Zamawiający informuje, iż jest możliwe odłączenie części napędów z obecnego systemu backupu i podłączenie ich do nowego systemu backupu.

III. Zamawiający wyznacza nowy termin składania ofert na dzień 26.07.2024 r.

Jednocześnie zmianie ulegają punkty 13, 14.2 oraz 14.3, SWZ, które otrzymują brzmienie:

- **13. Termin związania ofertą**

  Wykonawca będzie związany ofertą przez okres 30 dni, tj. do dnia **24.08.2024 r.** Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

  (…)

- **14.2. Termin składania ofert upływa w dniu 26.07.2024 r. o godz. 12:00**
- **14.3. Otwarcie ofert nastąpi w dniu 26.07.2024 r. o godzinie 12:05.**

Powyższe zmiany należy uwzględnić przy składaniu ofert. Pozostałe postanowienia SWZ pozostają bez zmian.

W wyniku dokonanej zmiany treści SWZ Zamawiający dokonał zmiany treści ogłoszenia. Ogłoszenie o zmianie ogłoszenia zostało opublikowane w Biuletynie Zamówień Publicznych w dniu 18.07.2024 r.

Załącznik:

Załącznik nr 1 do SWZ – Opis przedmiotu zamówienia.

Pełnomocnik Dyrektora PIG-PIB
ds. Zamówień Publicznych

Piotr Grochot

Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest:

1. **zadanie 1** - wdrożenie zaoferowanego oprogramowania w infrastrukturze zamawiającego do 30.11.2024 r.;
2. **zadanie 2** - dostarczenie w formie subskrypcji 500 licencji oprogramowania do backupu i archiwizacji danych przez okres 36 miesięcy. Licencja musi umożliwiać backup i archiwizację maszyn wirtualnych i serwerów fizycznych zamiennie. Wykonawca wraz z kluczem licencyjnym wskaże miejsce pobrania systemu;
3. **zadanie 3** – opieka techniczna przez okres 36 miesięcy równorzędnie z subskrypcją;

I. WYMAGANIA DLA WDROŻENIA SYSTEMU

1. Wykonawca zamówienia zainstaluje, uruchomi i skonfiguruje zaoferowany system z wykorzystaniem dotychczasowej infrastruktury systemu backupu posiadanej przez Zamawiającego, wskazanej w pkt. IV.
2. Wdrożenie zakończy się nie później niż 30 listopada 2024 r. Wdrożenie uznaje się za zakończone w momencie, w którym system backupu będzie umożliwiał wykonywanie kopii zapasowych zasobów wskazanych przez zamawiającego w pkt. V.
3. Zamawiający użytkuje obecnie rozwiązanie IBM Spectrum Protect w wersji 8.1.6. System wykorzystuje serwery, macierze dyskowe oraz bibliotekę taśmową opisane w pkt. IV.
4. Wykonawca skonfiguruje system w sposób umożliwiający wykonywanie kopii zapasowych zasobów opisanych w pkt. V.
5. Zamawiający wymaga dostępności do posiadanych backupów w trakcie procesu migracji.
6. Zamawiający wymaga, aby konfiguracja dostarczonego systemu przewidywała:
   - tworzenie i przechowywanie kopii podstawowej w lokalizacji Jagiellońska,
   - replikę kopii zapasowych w lokalizacji Kraków,
   - tworzenie kopii offline z wykorzystaniem biblioteki taśmowej w lokalizacji Jagiellońska.
7. Zamawiający wymaga, aby Wykonawca przed zakończeniem wdrożenia wykonał testy odtworzenia backupu z kopii podstawowej, repliki backupu oraz backupu offline w infrastrukturze Zamawiającego.
8. Zamawiający wymaga, aby Wykonawca opisał procedury odtwarzania backupu z wszystkich rodzajów kopii zapasowych zgodnie z najlepszymi praktykami.
9. Wykonawca przeszkoli wskazanych pracowników Zamawiającego w zakresie podstawowej administracji systemem: instalacja agentów, tworzenie i odtwarzanie kopii zapasowych, monitorowanie statusu systemu, tworzenie harmonogramów, podłączanie nowych urządzeń typu storage.

II. WYMAGANIA FUNKCJONALNE DLA OPROGRAMOWANIA

Wymagania ogólne
1. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5
2. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na platformach wirtualizacyjnych Vmware i Hyper-V
3. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania
4. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
5. Oprogramowanie musi przechowywać dane w formacie, których odzyskanie nie wymaga obecności bazy danych z metadanymi deduplikowanych bloków.
6. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
7. Utrata bazy deduplikatów używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Dane muszą być zapisane w formie pozwalającej na odtworzenie danych w przypadku utraty bazy deduplikatów.
8. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

9. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.
10. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
11. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)
12. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
13. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
14. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
15. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
16. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą dostępu do zaszyfrowanych danych.
17. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
18. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Wymagania RPO
19. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking dla minimum Vmware i Hyper-V.
20. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
21. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u poprzez konfigurację dopuszczalnego poziomu latencji lub zdefiniowanie pasma przepustowości dla backupu (throtling).
22. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.
23. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
24. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.
25. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
26. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
27. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
28. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
29. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
30. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO
31. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana minimum dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
32. Dodatkowo minimum dla środowiska vSphere oraz Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory oraz chmura publiczna)
33. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor.
34. Oprogramowanie musi pozwalać na udostępnienie pojedynczego dysku z kopii zapasowej dla wybranej działającej maszyny wirtualnej vSpehre
35. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB bezpośrednio ze skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.
36. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków

37. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
38. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
39. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
40. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
41. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
42. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji.
43. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects oraz pozwalać na odtworzenie haseł.
44. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.
45. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.
46. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.
47. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
48. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
49. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
50. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
51. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
52. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka
53. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, chmura publiczna)
54. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
55. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
56. Oprogramowanie musi umożliwiać integrację z minimum trzema różnymi dostawcami oprogramowania antywirusowego w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych.
57. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Środowiska fizyczne
58. Rozwiązanie musi wykonywać kopię zapasową systemu Windows, Linux oraz Unix (AIX) działającego na serwerze fizycznym wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego
59. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych
60. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE
61. Rozwiązanie musi wspierać system operacyjny macOS
62. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix
63. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster

64. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów
65. Rozwiązanie musi wspierać backup podłączonych dysków USB
66. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym
67. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)
68. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone
69. Rozwiązanie musi wspierać kontrolę pasma sieciowego
70. Oprogramowanie musi oferować możliwość ograniczenia wykonywania backupów tylko do konkretnych klas adresowych.
71. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft
72. Rozwiązanie musi wspierać technologię BitLocker
73. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania
74. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych
75. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych
76. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.
77. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych maszyn wirtualnych Vmware bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform
78. Rozwiązanie musi wspierać szyfrowanie
79. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
80. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych
Monitoring
81. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V
82. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
83. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
84. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
85. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
86. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
87. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
88. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
89. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
90. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
91. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
92. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
93. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
94. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4
Raportowanie

95.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
96.	System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
97.	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
98.	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
99.	System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
100.	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
101.	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
102.	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
103.	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
104.	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
105.	System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
106.	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
107.	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
108.	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
109.	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
110.	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
111.	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

III. WYMAGANIA DLA OPIEKI TECHNICZNEJ

1. Wykonawca będzie świadczyć pomoc telefoniczną, mailową, osobistą w siedzibie Zamawiającego lub zdalną (przy wykorzystaniu dedykowanego połączenia VPN) przy realizowaniu zadań związanych z administrowaniem, konfiguracją, migracją danych systemu backupu, poprzez udzielanie informacji technicznych, niezbędnych do prawidłowego działania systemu.
2. Wszelkie usługi opieki technicznej będą świadczone w dni robocze w godzinach 7 – 17.
3. Czas reakcji w przypadku problemów w zakresie administrowania systemem kopii zapasowych wynosi 24 godziny, natomiast rozwiązanie problemów nastąpi nie później niż 48 godzin od chwili jego telefonicznego lub elektronicznego (email/portal) zgłoszenia.
4. Wykonawca będzie świadczyć pomoc przy konfiguracji i instalacji nowych klientów systemu backupu, konfiguracji nowych harmonogramów.
5. Wykonawca będzie monitorować wszystkie elementy środowiska kopii zapasowych opisane w pkt. IV. W przypadku stwierdzenia zagrożeń w tym zakresie, Wykonawca poinformuje wskazanych w umowie pracowników Działu Informatyki PIG-PIB o wykrytych nieprawidłowościach. Monitorowanie będzie realizowane z wykorzystaniem narzędzi zdalnego, szyfrowanego dostępu do serwerów środowiska kopii zapasowych.
6. W przypadku awarii dowolnego elementu systemu wymienionego w pkt. IV, reakcja nastąpi nie później niż 24 godziny od chwili zgłoszenia telefonicznego lub elektronicznego (email/portal).. Wykonawca przeprowadzi diagnostykę i zaproponuje właściwe działania w terminie nie dłuższym niż 48 godzin od chwili zgłoszenia telefonicznego lub elektronicznego (email/portal). Zamawiający zrealizuje naprawę na podstawie posiadanych odrębnych umów serwisowych.
7. W przypadku awarii niezwiązanych z elementami systemu wymienionymi w pkt. IV, reakcja nastąpi nie później niż 24 godziny, a rozwiązanie problemu nastąpi nie później, niż w ciągu 48 godzin od chwili jego zgłoszenia telefonicznego lub elektronicznego (email/portal).

8. W przypadku, gdy przyczyną awarii jest urządzenie nie będące elementem systemu, Zamawiający uzna zgłoszenie za zrealizowane i dokona naprawy urządzenia na podstawie odrębnych umów serwisowych.
9. Na koniec każdego kwartału w ramach trwającej umowy, Wykonawca dostarczy pocztą elektroniczną raport, który będzie zawierał, co najmniej: status środowiska, zajętość zasobów wykorzystywanych do składowania kopii zapasowych, opis usuniętych problemów, przyrost zajmowanej przestrzeni w stosunku do stanu bezpośrednio po wdrożeniu systemu.
10. Wszystkie zidentyfikowane przez Wykonawcę problemy wynikające z błędów oprogramowania, zostaną przekazane przez niego do producenta oprogramowania.
11. Przed rozpoczęciem świadczenia usługi wsparcia zostanie zweryfikowana i zaktualizowana posiadana dokumentacja (szkic architektury, adresy IP, itp);
12. W przypadku dokonania zmian w architekturze systemu w okresie obowiązywania umowy, Wykonawca zaktualizuje dokumentację, o której mowa w ppkt 11 powyżej.

IV. ELEMENTY INFRASTRUKTURY BACKUPU

1. Zamawiający wymaga wdrożenia systemu na dotychczas wykorzystywanej infrastrukturze systemu backupu, na którą składają się:
   - serwer DELL EMC R640: Intel Xeon 4116, 64GB RAM, 512GB HDD
   - serwer DELL PowerEdge R650: Intel Xeon 4310, 512GB RAM, 480GB HDD – (nowy serwer pod instalację nowego systemu backup'u)
   - serwer Eterio 125 RE1: Intel Xeon 4214R, 32GB RAM, 2TB SSD (lokalizacja Kraków – replika)
   - macierz IBM FS5035 (lokalizacja Warszawa serwerownia główna – kopia podstawowa, o pojemności 200TB)
   - macierz IBM FS5035 (lokalizacja Kraków – replika, o pojemności 200TB)
   - biblioteka taśmowa HPE MSL6480 (lokalizacja Warszawa serwerownia główna – kopia off-line, o pojemności 1,2PB)
   - macierz QSAN XS5226 (niewykorzystywana produkcyjnie, dostępna jako ew. tymczasowy storage na potrzebny migracji do nowego systemu – o pojemności 220TB)
2. Lokalizacje Warszawa serwerownia główna i Kraków połączone są siecią światłowodową 10 Gbps łączem symetrycznym.

V. ZASOBY

1. Zamawiający posiada środowisko wirtualne Vmware składające się z 25 hostów pracujących pod kontrolą Vmware 6.7.0.
2. Zamawiający posiada środowisko wirtualne OLVM składające się z 4 hostów pracujących pod kontrolą OLVM w wersji 4.4.10.7
3. Zamawiający posiada serwery plików Microsoft Windows Server w wersji 2012, 2016 i 2019
4. Zamawiający posiada serwery bazodanowe: Oracle Database, Microsoft SQL Server, PostgreSQL, MariaDB
5. Zamawiający posiada serwery pocztowe: Exchange w wersji 2016.
6. Zamawiający posiada 500 serwerów (wirtualnych i fizycznych)