Załącznik nr 1 do SIWZ

Opis przedmiotu zamówienia

A. Serwer – 2 szt.

Wymagania minimalne:

1. **Obudowa:**
   - Typu Rack, wysokość maksimum 1U;
   - Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack;
2. **Płyta główna:**
   - Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów dwudziestoośmiordzeniowych;
   - wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3000GB pamięci RAM DDR4 2966 Mhz;
   - Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM;
   - Minimum 2 sloty dla dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express - nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera);
   - Minimum 2 wolne sloty PCI Express x8 do dalszej rozbudowy serwera, sloty aktywne;
3. **Procesor:**
   - Obsługa procesorów minimum 28-rdzeniowych;
   - Zainstalowane minimum dwa procesory 8-rdzeniowe taktowane podstawowym zegarem 2,5Ghz osiągające w oferowanym modelu serwera wynik SPECrate 2017_int_base co najmniej 97 punktów. Wynik dla oferowanego serwera z oferowanymi procesorami musi być dostępny na stronie spec.org
4. **Pamięć RAM:**
   - Zainstalowane 128GB pamięci RAM typu DDR4 Registered, 2966Mhz w kościach o pojemności 32GB;
   - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC lub równoważnej;
   - Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM;
5. **Kontroler RAID:**
   - Zainstalowany kontroler RAID 0,1;
6. **Dyski twarde:**
   - Zainstalowane 2 dyski SSD minimum 480GB SATA o parametrze DWPD minimum 3,5 dyski hotplug;
   - Minimum 8 wnęk dla dysków twardych Hotplug 2,5;
7. **Napędy zintegrowane:**
   - Wbudowany fabrycznie wewnętrzny napęd Blue-ray (odczyt/zapis) (dopuszcza się dostarczenie napędu zewnętrznego pod warunkiem objęcia serwisem o jednakowych parametrach z wymaganymi dla całego serwera)
8. **Kontrolery LAN:**
   - Jedna dwuportowa karta 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;

- Dodatkowa osobna karta 4x1Gbit/s, niezajmująca slotu PCI Express (dopuszcza się instalację kart w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilością slotów PCI Express)

9. **Kontroler FC:**
   - Jedna dwuportowa karta FC x16Gb Emulex;
10. **Porty:**
    - Zintegrowana karta graficzna ze złączem VGA;
    - 2x USB 3.0 dostępne na froncie obudowy
    - 2x USB 3.0 dostępne z tyłu serwera
    - 1x USB 3.0 wewnątrz serwera
    - Dodatkowe złącze VGA dostępne z przodu serwera;
    - Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;
11. **Zasilanie:**
    - Redundantne zasilacze hotplug o mocy minimum 800W, o sprawności 94% (tzw klasa Platinum)
    - Redundantne wentylatory hotplug;
12. **Zarządzanie:**
    - Wbudowane diody informacyjne informujące o stanie serwera
    - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Możliwość przejęcia konsoli tekstowej
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
- Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych)
- Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera)
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
- Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB
- Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB);
- Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania;

- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;
- Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);
- Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;
- karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie producenta serwera). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera;
- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web (także SSL, SSH)
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
- Zarządzanie alarmami (zdarzenia poprzez SNMP)

13. **Wspierane OS:**
    - Windows 2019 Hyper-V, Windows 2016 Hyper-V, VMWare, Suse, RHEL
14. **Oprogramowanie systemowe wraz z licencjami dostępowymi:**
    - system operacyjny spełniający poniższe warunki minimalne:
    - System operacyjny musi być przeznaczony do zastosowań serwerowych w Centrach danych i środowiskach chmur o wysokim stopniu wirtualizacji
    - System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta

- Warunki licencjonowania systemu operacyjnego muszą zezwalać na zmianę wersji systemu operacyjnego na niższą z zachowaniem wsparcia technicznego oraz na przeniesienie licencji systemu operacyjnego na inny fizyczny serwer
- W ramach dostarczonej licencji na system operacyjny musi być zawarta możliwość instalacji oprogramowania na serwerze wieloprocesorowym
- System operacyjny musi mieć możliwość obsługi co najmniej 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych)
- Obsługa pamięci RAM w wysokości przynajmniej 24TB
- Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania co najmniej przez 3 lat
- Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny
- System operacyjny musi mieć możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP)
- Licencja na system operacyjny musi być bez ograniczeń czasowych
- Licencja musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i nielimitowanej ilości środowisk wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji
- Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej
- System operacyjny musi wspierać projektowanie skalowalnych systemów pamięci masowej o wysokiej dostępności budowanych w oparciu o fizyczne hosty
- System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów
- Wszystkie narzędzia i usługi wykorzystywane w systemie operacyjnym powinny być rozwiązaniem jednego producenta
- System operacyjny musi pozwalać na obsługę pamięci USB jako monitora klastra oraz uaktualnienia stopniowego systemu operacyjnego klastra
- System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień
- System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6
- System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny
- System operacyjny musi posiadać możliwość uruchomienia serwera usług terminalowych
- System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu
- System operacyjny musi posiadać domyślną obsługę PowerShell 5.1
- System operacyjny musi posiadać funkcję magazynu danych definiowanego programowo
- Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte musza być dostarczoną licencją i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

- Dostarczona licencja na system operacyjny musi obejmować wszystkie rdzenie procesorów w dostarczonych w ramach postępowania serwerach, zgodnie z polityką licencjonowania producenta oprogramowania.
- Zamawiający dopuszcza, aby wersja systemu operacyjnego oraz licencje dostępowe były w wersji edukacyjnej lub akademickiej;
- Zamawiający wymaga, aby wraz z systemem operacyjnym zostało dostarczone sumarycznie 80 szt. licencji dostępowych dla urządzeń;

15. **Gwarancja i wsparcie:**

- Minimum 36 miesięcy gwarancji producenta serwera w trybie onsite z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime);
- Serwer musi być zaoferowany z serwisem producenta serwera, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego;
- Serwis musi umożliwiać konfigurację automatycznego powiadamiania serwisu producenta (otwieranie zgłoszenia serwisowego wg obowiązującego SLA) o przewidywanej bądź istniejącej usterce;
- Dostępność części zamiennych przez 5 lat od momentu zakupu serwera;
- Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;

16. **Dokumentacja:**

- Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty).
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;
- Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
- Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt na terenie Polski został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu;
- Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;

B. Macierz dyskowa – 1 szt.

Wymagania minimalne:

1. Macierz musi być wyposażona w co najmniej jedną parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe macierzy bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami (nie dopuszcza się żadnych połączeń typu IP/LAN poprzez zewnętrzne switche, główki, itp.);
2. Macierz posiada architekturę modułową dla instalacji kontrolerów, portów komunikacyjnych, oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski;
3. Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w standardowej szafie rack 19”
4. Zajętość kompletnej macierzy z modułami dyskowymi i modułami kontrolerów w oferowanej konfiguracji -maksymalnie 5U szafie rack.
5. Macierz zawiera łącznie minimum:
   a. 14 dysków 2,5” SAS 12G 10k RPM o pojemności minimum 2400GB każdy;
   b. Macierz w oferowanej konfiguracji musi posiadać minimum 10 wolnych wnęk na instalację dysków 2,5” SAS;
6. Macierz musi być wyposażona w minimum:
   a. 2 aktywne porty FC 16Gb przypadające na każdy z kontrolerów;
7. Każdy skonfigurowany moduł kontrolerów i/lub dyskowy musi posiadać nadmiarowy układ zasilania i chłodzenia zapewniający ciągłą pracę całej konfiguracji macierzy bez ograniczeń czasowych i wydajnościowych w przypadku usterki pojedynczego zasilacza lub elementu chłodzenia;
8. Macierz musi umożliwiać rozbudowę i jednoczesne podłączenie i używanie modułów dyskowych dla dalszej rozbudowy w co najmniej trzech wariantach:

   a. maksimum 2U przy gęstości upakowania minimum 24 dysków 2,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, NL-SAS,SSD w pojedynczej półce);

   b. maksimum 2U przy gęstości upakowania minimum 12 dysków 3,5” typu hotplug lub 4U przy gęstości upakowania minimum 24 dyski 3,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, NL-SAS,SSD);

   c. maksimum 4U przy gęstości upakowania minimum 60 dysków 3,5” typu hotplug (jednoczesna obsługa dowolnej kombinacji dysków SAS, NL-SAS,SSD);

   Wymaga się aby macierz umożliwiała jednoczesne podłączenie i użycie dowolnego rodzaju i kombinacji półek dyskowych typu a, b, c; (np. jednoczesne użycie półek gęstego upakowania typu c. i półek 2U dla dysków 2,5” typu a. w jednej macierzy)
9. Wszystkie zewnętrzne połączenia kablowe pomiędzy modułami muszą zapewniać komunikację nawet w przypadku awarii dowolnej z półek ze wszystkimi pozostałymi półkami/dyskami.
10. Połączenia kablowe SAS 12G pomiędzy modułami muszą zapewniać przepustowość minimum 48Gb/s w ramach pojedynczego połączenia.

11. Model oferowanej macierzy obsługuje minimum 220 dysków wykonanych w technologii hot-plug bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami;
12. Kontrolery macierzy obsługują tryb pracy w układzie active-active lub mesh-active. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami.
13. Każdy z kontrolerów macierzy posiada po minimum 64 GB pamięci podręcznej Cache – zawartość pamięci Cache musi być identyczna dla wszystkich kontrolerów macierzy.
14. Macierz w dostarczonej konfiguracji musi obsługiwać deduplikację i kompresję danych na dyskach wbudowanych w macierzy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie oraz niezależnie na poziomie każdego LUN:
    a. Sama kompresja wybranego LUN;
    b. Kombinacja technologii kompresji i deduplikacji wybranego LUN;
    c. Brak użycia technologii kompresji i deduplikacji dla wybranego LUN;

    Jeżeli do uruchomienia wymaganych funkcjonalności deduplikacji i kompresji są wymagane jakiekolwiek licencje lub elementy hardware wymaga się ich dostarczenia dla maksymalnej obsługiwanej przez macierz pojemności. Deduplikacja i kompresja musi być wspierana przez macierz na dowolnym typie obsługiwanych dysków – co najmniej NL-SAS, SAS, SSD.

    Mechanizmy deduplikacji i kompresji muszą być realizowane w tzw. Trybie „Online" to znaczy dane zapisywane na nośniki danych muszą być zapisywane przez kontrolery macierzy od razu w postaci skompresowanej/zdeduplikowanej bezpośrednio w trakcie zapisu danych przez macierz. Dopuszcza się technologię kompresji i deduplikacji w trybie tzw. „Offline" (czyli po uprzednim zapisaniu danych na pośredniczącą warstwę dysków w postaci nie-zdeduplikowanej i/lub nie-skompresowanej) przy wykorzystaniu dedykowanego cache dyskowego SSD pod warunkiem dostarczenia dodatkowej pojemności dysków SSD w konfiguracji RAID 6 lub RAID 10 o pojemności użytecznej minimum równej 25% sumarycznej wymaganej pojemności RAW macierzy (z uwagi na konieczność zachowania odpowiedniej wydajności przy kilkukrotym wzroście pojemności i operacji na macierzy w trakcie cyklu wieloletniego użytkowania sprzętu);
15. Macierz musi być wyposażona zabezpieczenie stanu pamięci cache np. na wypadek awarii zasilania – zapis stanu pamięci cache na dyski flash lub równoważny nośnik nie wymagający zasilania. Czas przechowywania kopii pamięci flash nie może być ograniczony czasowo.
16. Macierz musi umożliwiać wymianę minimum 1 kontrolera bez konieczności wyłączania zasilania całego urządzenia.
17. Macierz posiada minimum 4 dedykowane interfejsy RJ-45 Ethernet 1Gb/s dedykowane dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy.
18. Każdy z kontrolerów macierzy wyposażony co najmniej w procesor wykonany w technologii wielordzeniowej z minimum 8 rdzeniami.
19. Każdy kontroler macierzy pozwala na konfigurację interfejsów niezbędnych dla współpracy w sieci LAN, FC SAN oraz NAS.
20. Dla komunikacji blokowej I/O z serwerami oferowany model macierzy wyposażony w oferowaną ilość

kontrolerów musi obsługiwać co najmniej następujące protokoły i porty:

a. Możliwość instalacji minimum 8 portów SAS 12Gbit/s

b. Możliwość instalacji minimum 16 portów FC 16Gbit/s

c. Możliwość instalacji minimum 8 portów iSCSI 10 Gbit/s SFP+ lub RJ-45

d. Możliwość instalacji minimum 8 portów iSCSI 1 Gbit/s SFP+ lub RJ-45

Musi istnieć możliwość jednoczesnego wykorzystania różnych typów interfejsów.

21. Oferowany model macierzy umożliwia wymianę portów do transmisji danych na porty obsługujące protokoły: iSCSI 1 Gb/s, iSCSI 10Gb/s, FC 16Gb/s, FC 32Gb/s, SAS 12G. Wymiana portów nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych.
22. Dla komunikacji plikowej NAS z serwerami oferowany model macierzy wyposażony w oferowaną ilość kontrolerów musi obsługiwać co najmniej następujące protokoły i porty: CIFS, NFS oraz interfejsy Ethernet 1Gbit/s i 10Gbit/s. Oferowany model macierzy musi umożliwiać jednoczesne użytkowanie portów do komunikacji blokowej i plikowej.
23. Oprogramowanie do zarządzania zintegrowane jest z systemem operacyjnym macierzy zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS oraz NFS (nie dopuszcza się tzw główek czy dodatkowych serwerów podłączonych do macierzy w celu realizacji obsługi dostępu protokołami CIFS i NFS do danych znajdujących się na macierzy).
24. Macierz jest wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych.
25. Macierz obsługuje co najmniej następujące poziomy RAID: 0, 1 ,1+0 , 5 , 50, 6
26. Oferowana macierz wspiera co najmniej następujące typy dysków hot-plug:

    - dyski elektroniczne SSD SAS o pojemności minimum 30TB ;

    - dyski elektroniczne SSD SAS SED lub FDE;

    - dyski mechaniczne HDD SAS, NL-SAS;

    - Wszystkie dyski wspierane przez oferowany model macierzy wykonane są w technologii hot-plug i posiadają podwójne porty SAS obsługujące tryb pracy full-duplex
27. Model macierzy pozwala na instalację dysków hot-plug w formacie 2,5” i 3,5”.
28. Macierz umożliwia skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach:

    - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID

    - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID lub zapewnia możliwość skonfigurowania równoważnej przestrzeni zapasowej.

29. W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk.
30. Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą odbywa się w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. Zdalne zarządzanie macierzą odbywa się bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.
31. Wbudowane oprogramowanie macierzy obsługuje połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI.
32. Macierz wyposażona jest w system kopii migawkowych umożliwiających wykonanie minimum 2048 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy.
33. Macierz umożliwia zdefiniowanie minimum 4096 woluminów LUN.
34. Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy.
35. Macierz umożliwia aktualizację oprogramowania wewnętrznego, kontrolerów i dysków bez konieczności wyłączania macierzy i bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych serwerów.
36. Macierz umożliwia dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupę dyskową.
37. Macierz posiada wsparcie dla systemów operacyjnych: MS Windows Server 2016 i 2019, SuSE Linux, RedHat Linux,
38. Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath dla połączeń FC i iSCSI.
39. Macierz obsługuje woluminy logiczne o maksymalnej pojemności minimum 16TB.
40. Macierz umożliwia obsługę mechanizów QoS (ang. Quality of Services) czyli nadawanie priorytetów obsługi transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów.
41. Macierz umożliwia rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD.
42. Macierz musi pozwalać na integrację macierzy w środowiskach Vmware w zakresie obsługi mechanizmów: Vmware VAAI, Vmware VVOL, Vmware VASA, Vmware MultiPath IO.
43. Wraz z macierzą należy zapewnić wsparcie dla mechanizmów Offloaded Data Transfer i Space Reclamation.
44. Macierz musi obsługiwać mechanizmy Thin Provisioning. Jeżeli taka funkcjonalność wymaga

dodatkowych licencji to należy je dostarczyć wraz z macierzą dla maksymalnej pojemności dyskowej oferowanej macierzy.

45. Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering).Mechanizm ten musi być obsługiwany przy trzech różnych technologiach dyskowych równoczesnie: SSD, SAS, NLSAS. Macierz musi pozwalać na definiowanie minimum 120 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy. Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB. Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O. Zamawiający nie wymaga dostarczenie licencji na wymienioną funkcjonalność. Licencja nie jest przedmiotem niniejszego postępowania.
46. Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC oraz iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych jest zapewniona z poziomu oprogramowania wewnętrznego macierzy. Zamawiający nie wymaga dostarczenie licencji na wymienioną funkcjonalność. Licencja nie jest przedmiotem niniejszego postępowania.
47. Model oferowanej macierzy musi wspierać rozwiązania klasy „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej.
48. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać poziomy RAID: 1,10,5, 6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną.
49. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover).
50. Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover).
51. Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback).
52. Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.
53. Funkcjonalność „wysokiej dostępności" musi wspierać dwukierunkowe przełączanie macierzy podstawowej na zapasową tj. przypadek, gdy każda z tych macierzy obsługuje własne środowisko produkcyjne, a rolę jej macierzy zapasowej pełni druga z macierzy.

54. Macierz dyskowa objęta jest minimum 36 miesięcznym okresem gwarancji producenta z gwarantowaną skuteczną naprawą w miejscu instalacji urządzenia najpóźniej następnego dnia roboczego od zgłoszenia usterki. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email (w ofercie należy podać dedykowany adres email serwisu producenta macierzy do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. W formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować dedykowany numer telefonu do obsługi zgłoszeń serwisowych. Wymagane jest oświadczenie Producenta oferowanej macierzy, iż wymagany poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta macierzy na potrzeby oferty w niniejszym postępowaniu

55. Serwis gwarancyjny obejmuje dostęp do poprawek i nowych wersji firmware, które są elementem zamówienia przez cały okres obowiązywania gwarancji.

56. Macierz musi być zaoferowana z serwisem producenta macierzy, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego. Serwis taki musi dotyczyć wszystkich oferowanych półek dyskowych i przewidywać ich uzupełnienie do maksymalnej pojemności poprzez dodanie dowolnych typów obsługiwanych dysków przez macierz bez konieczności ponoszenia żadnych dodatkowych kosztów przez Zamawiającego z tytułu gwarancji „pozostawienie dysku" dla tych dysków zainstalowanych w macierzy jak i dodatkowych dysków możliwych do zainstalowania w obrębie oferowanych półek dyskowych. Wymagane jest oświadczenie Producenta oferowanej macierzy, iż wymagany poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta macierzy na potrzeby oferty w niniejszym postępowaniu;

57. Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje;

58. Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system

serwisowy macierzy. W celu zapewnienia odpowiedniego SLA jako element odbioru technicznego macierzy wymaga się dostarczenia oświadczenia Producenta macierzy, iż odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta macierzy celem świadczenia proaktywnego wsparcia/kontaktu w przypadku nastąpienia usterki w Polsce. (Dane zostaną podane przez Zamawiającego z minimum 14 dniowym wyprzedzeniem przed odbiorem sprzętu).

59. Oferowana macierz musi być fabrycznie nowa, Macierz pochodzi z legalnego kanału sprzedaży producenta na terenie Polski i reprezentuje model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych.
60. Urządzenie wykonane jest zgodnie z europejskimi dyrektywami RoHS i WEEE.
61. Przed podpisaniem protokołu ilościowo-jakościowego Wykonawca dostarczy pisemne potwierdzenie wykupienia i uruchomienia gwarancji producenta macierzy obowiązującej na terenie Polski, zgodnej co najmniej z wymaganiami specyfikacji i ze złożoną przez niego ofertą.

C. Przełącznik Fibre Channel – 2 szt.

Wymagania minimalne:

1. **Ilość portów FC:**
   - Łączna ilość aktywnych portów FC – 8 z możliwością rozszerzenia do 24 szt. portów 32Gbit/s Fibre Channel. Rozbudowa nie może odbywać się poprzez zakup elementów modułów sprzętowych, jedynie poprzez zakup licencji i wkładek;
   - W pełni rozbudowany przełącznik nie może zajmować w szafie RACK więcej niż 1U;
2. **Przepustowość portu:**
   - Porty uniwersalne o przepustowości 32GB/s, z obsługą przepustowości 4Gbit/s, 8Gbit/s i 16 Gbit/s z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex dla wszystkich wspieranych przepustowości;
3. **Interfejsy optyczne:**
   - Moduły do transmisji światłowodowej z prędkością min. 16Gbit/s poprzez kabel światłowodowy wielomodowy (Short-Wavelenght) z interfejsem LC, liczba modułów dostosowana do liczby aktywnych portów, możliwość pracy z prędkością min. 16Gbit/s.
4. **Inne funkcje i wyposażenie:**

- Obsługa trybów pracy portów FC: D_Port, E_port, F_port, N-Port;
- Obsługa funkcji PoD (Ports on Demand) przydziału licencji dla aktywnych portów FC;
- Aktywne licencje:
  - Webtools,
  - Full Fabric (z obsługą do min. 239 przełączników FC),
  - Zoning,
  - Ports on Demand.
- Możliwość zdalnej aktualizacji firmware'u switcha;
- Możliwość rozbudowy o funkcjonalności:
  - FabricVision,

- Extended Fabric,
- Inter Switch Link (ISL) z przepustowością maks. 256 Gb/s /ISL.

- Dedykowany interfejs RJ-45 min 10/100/1000 Mb/s do zarządzania poprzez sieć Ethernet;

- Możliwość zarzadzania typu in-band poprzez Fibre Channel;

- Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy, dedykowany port USB umożliwiający upgrade FW i zapis logów;

- Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia;

- Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych min. 128-bit SSL oraz poprzez usługę SSH;

- Zarządzanie poprzez konsole znakową tzw. CLI;

- Wsparcie dla protokołu SNMP v.3;

5. **Kable:**
   - Urządzenie należy dostarczyć wraz kablami LC-LC o długości min. 5 m. – sumarycznie minimum 10 sztuk na potrzeby projektu;
6. **Typ obudowy:**
   - Wysokość przełącznika 1U w systemie montażu w szafie typu rack 19". Szyny montażowe w zestawie. Wraz z przełącznikiem należy dostarczyć również perforowany panel 1U;
7. **Zasilanie:**
   - Zasilanie z sieci prądu przemiennego o napięciu w zakresie 90- 264V/50-60Hz V, maksymalny pobór mocy podczas pracy urządzenia 77W
8. **Gwarancja, inne:**
   - Urządzenie musi być objęte gwarancją producenta na okres 36 miesięcy z reakcją w miejscu instalacji urządzenia najpóźniej w następnym dniu roboczym od zgłoszenia;
   - Przełącznik musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce ;
   -Możliwość zgłaszania usterek mailowo i telefonicznie 7 dni w tygodniu, całodobowo, również w dni świąteczne. Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email (w ofercie należy podać dedykowany adres email serwisu producenta macierzy do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny);
   - Wymagane oświadczenie producenta, że oferowany do przetargu sprzęt spełnia wymogi gwarancyjne;

D. Biblioteka taśmowa wraz z oprogramowaniem- 1 szt.

Wymagania minimalne:

1. **Obudowa:**
   - Kompletne urządzenie w oferowanej konfiguracji nie może zajmować więcej niż 3U zajętości w szafie rack.
   - Oferowana biblioteka musi posiadać zainstalowany magazynek lub magazynki umożliwiające obsługę co najmniej 40 nośników LTO.
   - Biblioteka musi posiadać nadmiarowe zasilanie (minimum 2 zasilacze redundantne)
2. **Funkcje, możliwości rozbudowy:**
   - Biblioteka musi posiadać konstrukcje modułową umożliwiająca dalszą rozbudowę do spójnej obsługi minimum 280 taśm LTO oraz 20 napędów LTO (jedno urządzenie z pojedynczym punktem zarządzania).

- Moduły muszą posiadać kompletny zestaw akcesoriów (szyny montażowe, mocowania szyn montażowych) pozwalających na ich instalację w standardowej szafie przemysłowej RACK oraz posiadać redundantne zasilanie.
- Moduł główny biblioteki musi posiadać panel operatora wyposażony w wyświetlacz LCD pozwalający na wykonanie podstawowych operacji konfiguracji ustawień biblioteki, inwentaryzacji taśm, testowanie biblioteki, robotyki i napędów, relokacji nośników taśmowych w ramach partycji, czyszczenie napędów z użyciem nośników czyszczących, sprawdzanie zawartości logów zbierających informacje o awariach sprzętowych i błędów w obsłudze napędów i nośników, konfiguracji parametrów koniecznych dla ustawienia zdalnego zarządzania biblioteką poprzez sieć LAN.
- Panel operatora musi posiadać możliwość blokady operacji konfiguracyjnych poprzez zabezpieczenie hasłem lub kodem PIN. Każdy moduł biblioteki musi posiadać możliwość wymiany lub uzupełniania nośników taśmowych bez przerywania pracy napędów taśmowych tzw. Mailslot.
- Biblioteka musi być wyposażona w minimum jeden interfejs Ethernet RJ-45 obsługujący prędkości transmisji 10/100/1000Mb/s dla zdalnego zarządzania biblioteką oraz w interfejsy USB wyprowadzone na front i tył obudowy głównego modułu biblioteki.
- Biblioteka taśmowa musi obsługiwać mechanizmy partycjonowania logicznego swoich zasobów z możliwością zdefiniowania minimum 2 partycji. Nie jest wymagane dostarczenie licencji dla aktywowania tej funkcjonalności.
- Biblioteka musi wspierać mechanizmy szyfrowania danych na nośnikach taśmowych LTO-6 i LTO-7 i LTO-8 z poziomu aplikacji do wykonywania kopii zapasowych.
- Biblioteka musi wspierać protokół KMIP (Key Management Interoperability Protocol) dla bezpiecznego przesyłania kluczy szyfrujących poprzez sieć LAN. Nie jest wymagane dostarczenie licencji dla aktywowania tej funkcjonalności dla zapisu i wgrywania parametrów konfiguracyjnych i/lub wgrywania nowego oprogramowania wewnętrznego elementów biblioteki.
- Biblioteka musi być wyposażona w czytnik kodów kreskowych pozwalający na automatyczną inwentaryzację zainstalowanych nośników taśmowych LTO posiadających etykiety z takim kodem, Każdy moduł biblioteki musi pozwalać na mieszaną konfigurację obsługiwanych napędów LTO, Wymagane jest dostarczenie konfiguracji z min. 1 aktywnym slotem na nośniki LTO 7.

3. **Napędy taśmowe:**
   - Biblioteka musi jednocześnie obsługiwać napędy taśmowe LTO-6, LTO-7 i LTO-8.
   - Biblioteka musi jednocześnie obsługiwać napędy LTO j.w. wyposażone w interfejsy FC 8Gb/s i SAS 6Gb/s.
   - Wymagane jest dostarczenie min. 1 napędów LTO7 FC. Wymagane jest dostarczenie 20 taśm LTO7 oraz minimum 1 taśmy czyszczącej LTO.
4. **Zarządzanie:**
   - Biblioteka musi pozwalać na administrację zdalnie poprzez sieć LAN w trybie Web-GUI z poziomu standardowej przeglądarki WWW.
   - Biblioteka musi obsługiwać komunikacje z szyfrowaniem transmisji protokołem SSL.
   - Biblioteka musi obsługiwać protokół SNMP v.1/2/3 oraz adresację zgodną ze standardem IPv.4 i IPv.6 dla modułu zdalnego zarządzania.
   - Biblioteka musi obsługiwać tryb automatycznego powiadamiania o błędach i zdarzeniach krytycznych poprzez wysyłanie wiadomości e-mail oraz poprzez wysyłanie komunikatów SNMP do uprawnionej stacji administratora obsługującej zarządzanie na platformie SNMP.

5. **Gwarancja, inne:**
   - Minimum 36 miesięcy gwarancji producenta biblioteki z reakcja na miejscu u Zamawiającego (wizyta serwisanta) na następny dzień roboczy od zgłoszenia.
   - Gwarancja musi być świadczona przez producenta biblioteki w miejscu instalacji biblioteki.
   - Producent biblioteki musi umożliwiać skuteczne zgłaszanie usterki trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia usterek muszą być akceptowane przez producenta zarówno drogą email (w ofercie należy podać dedykowany adres email serwisu producenta biblioteki do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna producenta, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Linia telefoniczna musi być czynna 24 godziny na dobę, 7 dni w tygodniu również w dni świąteczne. W formularzu ofertowym należy podać pełen adres internetowy strony producenta biblioteki, gdzie można zweryfikować dedykowany numer telefonu do obsługi zgłoszeń serwisowych.
   Wymagane jest oświadczenie Producenta oferowanej biblioteki, iż wymagany poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta na potrzeby oferty w niniejszym postępowaniu;
   - Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, w ciągu całego okresu gwarancji. Wraz z biblioteką należy zapewnić subskrypcję na bezpłatną aktualizację (możliwość bezpłatnego pobrania ze stron internetowych producenta) oprogramowania wewnętrznego biblioteki (tzw. firmware) w całym okresie obowiązywania gwarancji;
   - Urządzenie musi pochodzić z autoryzowanego kanału sprzedaży producenta na rynek Polski lub UE i musi reprezentować model z bieżącej linii produkcyjnej. Nie dopuszcza się użycia elementów i podzespołów biblioteki oferowanych jako refabrykowane, podemonstracyjne lub powystawowe.
6. **System backupowy (oprogramowanie do backupu):**
   - Pojęcie system wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie niezintegrowanych pomiędzy sobą wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji.
   - Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych lub pocztowych do archiwum (repozytorium dyskowe lub taśmowe) z pozostawieniem skrótów lub bez ich pozostawiania.
   - Jeśli przy danym punkcie wymogu występuje informacja „jako opcja" oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.
   - W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymogi podstawowe

1. Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych.

2. Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia.
3. Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą umożliwiać na zainstalowanie go: na serwerze fizycznym, klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V.
4. Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15 minut. Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego. Zamawiający udostępni jedynie licencje na system operacyjny Windows Standard 2016/2019 w ilości sztuk 1 oraz serwer backupowy z minimalnymi parametrami, które są wymagane do zainstalowania dostarczonego oprogramowania do backupu.
5. Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji.
6. Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich
7. System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów.
8. System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania
9. Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie
10. System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu.
11. System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej
12. Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ
13. Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe
14. System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP
15. Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania
16. System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN
17. System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi

umożliwiać przechowywanie danych po deduplikacji minimum do 200 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowych dysków czy macierzy dyskowej).

18. Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh
19. Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej centralnej bazie dedupplikacyjnej
20. Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych.
21. Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB.
22. System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji.
23. System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu.
24. Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej
25. System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych
26. System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie wykorzystuje bazę deduplikacyjną.
27. Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu.
28. System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną
29. System musi zapewniać zintegrowane logowanie dla użytkownika końcowego poprzez tzw. social media (minimum poprzez Google)
30. System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD.
31. System musi pozwalać na zarządzanie z poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH.
32. Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach

33. System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych)
34. System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail
35. Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu.
36. Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem
37. System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO
38. System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password
39. System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym – minimum dla
    - Safenet
    - Amazon Web Services (AWS) key management service
    - Microsoft Azure Key Vault
40. System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy
41. System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
    - Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane
    - Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot
    - Monitorowanie dużych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji
42. System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email.
43. System musi automatycznie wysyłać informacje o alertach, zdarzeniach oraz informacjach audytowych do syslog serwera
44. Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach
45. System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
    - Raport zmian/wzrostu środowiska systemu
    - Raport wykorzystania licencji
    - Raport wykonanych zadań backupowych
46. System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail
47. System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV

48. System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryterii:
    - Czas zadania dłuższy niż zadany
    - Ilość danych większa niż ….
    - Ilość danych mniejsza niż ….
    - Ilość nie zbackupowanych plików większa niż
    - Ilosc nie zbackupowanych plików większa niż …%
    - Wielkośc backupowanych danych wieksza niż …
49. Notyfikacje alertów muszą być wysyłane minimum poprzez mail.
50. Raport spełnienia wymogów SLA dla parametrów:
    - Ilości dodatkowych kopii backupowych
    - RTO
    - RPO
51. System musi zapewniać funkcjonalność wznawiania zadań backupowych.
52. System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych.
53. System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy
54. Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu
55. System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków
56. Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego.
57. System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych.
58. System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji.
59. System ma realizować procesy backupu oraz odzyskiwania danych.
60. System ma umożliwić tworzenie zadań backupowych w oparciu o kalendarz.
61. System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane backupowane i archiwizowane.
62. System musi realizować funkcjonalność weryfikacji wykonanych kopii.
63. System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
    - Windows: 2016/2012/2008/2003/10/8.1/8/7/Vista/XP
    - Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu

- Unix: AIX/Solaris
- OpenVMS

64. System musi umożliwiać (jako opcja) integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri, Kaminario, z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostepny nie tylko dla zasobów plikowych ale i aplikacji.
65. Dla producentów: NetApp, EMC i HDS system musi (jako opcja) umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze
66. System musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe i taśmowe
67. System powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon
68. System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows
69. System musi pozwalać na odtwarzanie tylko samych uprawnień do plików
70. System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL)
71. System (jako opcja) powinien umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryterii powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log.
72. Możliwość odtwarzania backupów plikowych poprzez udostepnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS
73. System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux
74. System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix
75. System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Red Flag Linux, Scientific Linux, Ubuntu, Slackware
76. System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris
77. System musi wspierać funkcjonalność odtwarzania fizycznego serwera do środowiska wirtualnego, minimum: dla serwera Windows do środowiska Vmware
78. System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.
79. System musi wspierać czołowe rozwiązania wirtualizacyjne: VMware, Hyper-V, Citrix Xen, RHEV, OracleVM, Docker, OpenStack, Huawei FusionCompute, Nutanix Acropolis, OpenShift. To znaczy musi posiadać dedykowanego agenta do backupu minimum całej maszyny wirtualnej bez konieczności instalowania agenta wewnątrz maszyny.
80. System musi wspierać wersje środowisk VMware 4.1, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7 poprzez integrację z vStorage API
81. Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS
82. System musi wspierać środowisko Xen: Citrix XenServer 6.0, 6.1, 6.2, 6.5
83. System musi wspierać środowisko Hyper-V dla:

- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012
- Microsoft Hyper-V Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Hyper-V Server 2012 R2
- Microsoft Windows Server 2016 (z Core Edition)
- Microsoft Hyper-V Server 2016 (z Core Edition)
- Microsoft Windows Server, version 1709 (z Core Edition)
- Microsoft Hyper-V Server, version 1709 (z Core Edition)

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

99. System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL
100. Dla minimum mySQL i PostgresSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego
101. Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle
102. Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio
103. Wsparcie dla backupu online dla minimum MS SQL Server 2016/2014/2012/2008/2005
104. Dedykowany agent bazodanowy dla backupu MS SQL na platformie Linux: Ubuntu, SuSe, RHEL
105. Możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML
106. Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore)
107. Dedykowani agenci (jako opcja) do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk
108. Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, mySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów
109. Możliwość backupu i odtwarzania (jako opcja) dokumentów dla Office 365
110. System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:
    - System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh
    - Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android
    - Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa.
    - System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i destopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny.
    - System musi oferować możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły)
    - Każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to:
        - ✓ Odtwarzanie własnych danych
        - ✓ Uruchomienie backupu
        - ✓ Wstrzymanie backupu
        - ✓ Możliwość zdefiniowania innego okna backupowego
        - ✓ Możliwość monitorowania postępu działania zadania
        - ✓ Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii

ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN)

- Zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane
- Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub)

111. Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych.
112. System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak:
    - Oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych.
    - Oprogramowanie musi obsługiwać strategię wielowarstwowego aktywnego archiwum. Na przykład, umożliwiać przenoszenie zarchiwizowanych plików pomiędzy różnorodnymi urządzeniami pamięci masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu przejrzystego jedno- krokowego odzyskiwania dla użytkowników końcowych.
    - Oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych.
    - Oprogramowanie musi wspierać proces archiwizacji bezpośrednio na taśmy.
    - Oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej.
    - Oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów
113. System musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili z skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling)
114. Oprogramowanie musi umożliwiać (jako opcja) raportowanie wszystkich zadań archiwizacyjnych i odtworzeniowych dla celów zgodności z przepisami/normami bezpieczeństwa (compliance).
115. System musi umożliwiać (jako opcja) pełnokontekstowe indeksowania treści danych dla wybranych typów plików, indeksacja musi odbywać się dla danych znajdujących się już w systemie.
116. System musi umożliwiać (jako opcja) przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji.
117. System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok….) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie

118. Musi istnieć dedykowany agent do backupu online aplikacji MongoDB
119. System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce, Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Unix i Linux
120. System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym
121. Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell
122. Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy
123. Agent do backupu systemów plikowych: Lustre, GlusterFS
124. Wsparcie dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O)
125. System musi zamierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum:
    - Identyfikacja taśm, które muszą być wyciągnięte z biblioteki
    - Identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej
    - Automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów
    - Identyfikacja i monitorowanie nośników (taśm) w trakcie transportu
126. Możliwość backupu skrzynek pocztowych Google i Google drive
127. Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy
128. System musi posiadać integrację z ServiceNow o funkcjonalnościach:
    - Dedykowany plugin do ServiceNow
    - Możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli Service Now

Wymogi dla licencjonowania

1. Sposób licencjonowania dla systemu musi opierać się na ilości serwerów/hostów – dla serwerów fizycznych, a dla środowisk wirtualnych na ilości maszyn wirtualnych lub fizycznych CPU wirtualizatorów podlegających zabezpieczeniu.
2. Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu
3. Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na nielimitowana ilość bibliotek taśmowych i napędów fizycznych.
4. Oferowana licencja musi pozwalać na nielimitowana budowę architektury systemu backupowego czy to w jednej czy w wielu lokalizacjach
5. W przypadku wielu lokalizacja licencja musi pozwalać na replikację danych po deduplikacji pomiędzy lokalizacjami
6. Do dostarczonych licencji jest wymagane 12 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień.
7. Zaoferowane licencje na system muszą zapewnić backup środowiska o wielkości:

- 4 CPU fizycznych wykorzystywanych przez system wirtualizacyjny.

E. Szafa teleinformatyczna wraz z zasilaniem awaryjnym - 1 szt.

Wymagania minimalne:

1. Szafa teleinformatyczna: 1 szt.

- Szafa rack o wysokości użytecznej 42U;
- Głębokość minimum 1200mm;
- Szerokość minimum 600mm;
- Wysokość maksimum 2105mm;
- Nośność certyfikowana szafy rack minimum 840 kg;
- Chłodzona pasywnie – perforacje (minimum 80% powierzchni czołowej) w drzwiach tylnych i przednich, umożliwiające instalację i poprawne chłodzenie urządzeń w trybie przód- tył (gorące powietrze wydmuchiwane z tyłu szafy);
- Drzwi przednie i tylne zamykane na zamek;
- Szafa musi być fabrycznie nowa;
- Wyposażona w co najmniej 2 niezależne listwy zasilające 1 fazowe, z których każda posiada minimum 10 gniazd zasilających typu IEC320 C13/C14 do podłączenia urządzeń zainstalowanych w szafie, oraz gniazdo podłączeniowe do zasilania zewnętrznego typu CEE 16A, jednofazowe;
- Szafa teleinformatyczna musi posiadać 36 miesięcy gwarancji producenta w trybie – onsite

2. Zasilanie awaryjne (UPS): 1 szt.

- UPS rack o wysokości max 3U razem z baterią;
- minimum 5KVA (4500W)
- minimum 6 gniazd IEC320 C13 (10A) do podłączenia urządzeń
- minimum 4 gniazda IEC320 C19 (16A) do podłączenia urządzeń
- dwie zarządzalne grupy dla gniazd zasilania urządzeń
- UPS zainstalowany w oferowanej szafie rack (wymagane odpowiednie szyny montażowe) i podłączony do jednej z listwa zasilających (możliwość podłączeni urządzeń zainstalowanych w szafie poprzez listwę zasilającą do UPS bez podtrzymania redundancji zasilania - po jednym zasilaczu z każdego;
- menu w postaci wyświetlacza LCD i przycisków kontrolujących
- UPS musi być wyposażony w kartę zarządzającą umożliwiającą zarządzanie zdalne przez sieć LAN (złącze RJ-45)
- UPS wraz z baterią musi posiadać 36 miesięcy gwarancji producenta w trybie – onsite

F. Urządzenie brzegowe - 1 szt.

Wymagania minimalne:

1. Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące

w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

2. **Redundancja, monitoring i wykrywanie awarii**

W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall;

Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych;

Monitoring stanu realizowanych połączeń VPN;

System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych;

3. **Interfejsy, Dysk, Zasilanie:**

System realizujący funkcję Firewall musi dysponować minimum:

- 16 portami Gigabit Ethernet RJ-45.
- 8 gniazdami SFP 1 Gbps.
- 2 gniazdami SFP+ 10 Gbps

System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB;

W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q;

System musi być wyposażony w zasilanie AC;

4. **Parametry wydajnościowe:**

W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 50.000 nowych połączeń na sekundę;

Przepustowość Stateful Firewall: nie mniej niż 10 Gbps;

Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps;

Wydajność szyfrowania IPSec VPN: nie mniej niż 10 Gbps;

Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps;

Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps;

Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 900Mbps;

5. **Funkcje Systemu Bezpieczeństwa:**

   W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

   - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection;
   - Kontrola Aplikacji;
   - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN;
   - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS;
   - Ochrona przed atakami - Intrusion Prevention System;
   - Kontrola stron WWW;
   - Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3;
   - Zarządzanie pasmem (QoS, Traffic shaping);
   - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP);
   - Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site;
   - Analiza ruchu szyfrowanego protokołem SSL;
   - Analiza ruchu szyfrowanego protokołem SSH;

6. **Polityki, Firewall:**

   Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

   System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

   - Translację jeden do jeden oraz jeden do wielu;
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP;

   W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN;

7. **Połączenia VPN:**

   System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

   - Wsparcie dla IKE v1 oraz v2;
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM);
   - Obsługa protokołu Diffie-Hellman grup 19 i 20;
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE;
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site;
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego;
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth;
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site;

   System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0;

- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta;

8. **Routing i obsługa łączy WAN:**

   W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego;
   - Policy Based Routingu;
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM;

   System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
9. **Zarządzanie pasmem:**

   System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
   Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
   System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
10. **Kontrola Antywirusowa:**

    Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
    System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
    System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
    System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
11. **Ochrona przed atakami:**

    Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
    System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
    Baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
    System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
    Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
    Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
12. **Kontrola aplikacji:**

    Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
    Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
    Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
    Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
13. **Kontrola WWW:**

    Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

14. **Uwierzytelnianie użytkowników w ramach sesji:**

System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

15. **Zarządzanie:**

Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

16. **Logowanie:**

Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
Musi istnieć możliwość logowania do serwera SYSLOG.

17. **Certyfikaty:**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.

- ICSA dla funkcji SSL VPN.

18. **Serwisy i licencje:**

    W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

    - Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

19. **Gwarancja oraz wsparcie:**

    System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.