ZP/UR/140/2019 Załącznik nr 1 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

(parametry i wymagania minimalne)

Przedmiotem zamówienia jest sprzedaż i dostawa oprogramowania oraz wyposażenia serwerowni Uniwersyteckiego Centrum Informatyzacji Uniwersytetu Rzeszowskiego.

W ramach realizacji przedmiotu umowy Wykonawca zobowiązany jest w szczególności do:

a) dostawy sprzętu wraz z montażem, instalacją, konfiguracją, uruchomieniem, wdrożeniem oraz w wymaganych przypadkach wykonanie koniecznych instalacji, w tym ułożenie kabli strukturalnych i montaż gniazd,
b) dostawy oprogramowania wraz z jego instalacją, konfiguracją i uruchomieniem,
c) zainstalowania, uruchomienia i wdrożenia infrastruktury serwerowej systemowo - narzędziowej kompatybilnej i bezawaryjnie współpracującej z posiadanymi przez Zamawiającego sprzętem i systemami, w tym systemem zarządzania uczelnią,
d) opracowania koncepcji technicznej, opis testów,
e) opracowania dokumentacji powykonawczej i zaleceń powdrożeniowych,
f) przeprowadzenia instruktarzów dla 5 pracowników Zamawiającego z zakresu:

- instalacji, konfiguracji i zarządzania środowiskiem oferowanego systemu wirtualizacji,
- instalacji, konfiguracji i zarządzania środowiskiem oferowanego systemu backupu,
- zarządzania środowiskiem oferowanego systemu zarządzania środowiskiem sieciowym.

g) bezpłatne konsultacje ze specjalistami drogą internetowa lub telefoniczna przez okres co najmniej 3 lat od dnia podpisania protokołu odbioru przedmiotu zamówienia dla danego etapu,
h) bieżąca konserwacja wynikająca z warunków gwarancji,
i) zapewnienie serwisu gwarancyjnego obejmującego przedmiot zamówienia,
j) na 1 miesiąc przed upływem terminu gwarancji, Wykonawca zapewnia pełny, bezpłatny przegląd okresowy całego dostarczonego sprzętu,
k) dostawa sprzętu fabrycznie nowego, nieużywanego,
l) dostawa oprogramowania komputerowego zakupionego w oficjalnym kanale sprzedaży, co oznacza zapewnienie stosownego pakietu usług gwarancyjnych, wsparcia techniczno – serwisowego kierowanego do użytkowników z obszaru Rzeczpospolitej Polskiej,
m) w przypadku dostarczenie oprogramowania komputerowego zapisanego na nośnikach, każdy z takich nośników musi być fizycznie nowy, posiadać kod aktywacyjny wraz z instrukcja aktywacyjną (oryginalnie zapakowany, zabezpieczony taśmą, nieposiadający śladów otwierania i użytkowania).
n) dostarczenie wraz z dostawą wszelkich niezbędnych dokumentów wymaganych przy tego typu sprzęcie tj. karta gwarancyjna, instrukcja obsługi w języku polskim, aprobata techniczna, certyfikaty, wszystkie dokumenty załączone do dostarczonego przedmiotu zamówienia muszą być sporządzone w formie drukowanej.
o) uwzględniania w toku realizacji przedmiotu zamówienia uwag i opinii Zamawiającego,

SZCZEGÓŁOWA SPECYFIKACJA

W ramach rozbudowy istniejącej infrastruktury informatycznej Uniwersytetu Rzeszowskiego należy dostarczyć fabrycznie nowy, nieużywany następujący sprzęt informatyczny i oprogramowanie oraz wykonać jego montaż, instalację, konfigurację i uruchomienie zgodnie z poniższymi minimalnymi wymogami i parametrami.

1. ETAP I: Oprogramowanie i wyposażenie serwerowni Uniwersyteckiego Centrum Informatyzacji – SPRZĘT o minimalnych parametrach:

Środowisko sprzętowe oparte o serwery działające w klastrze wirtualizacyjnym oraz serwer dyskowy:

1.1. Serwer dyskowy o następujących parametrach minimalnych – 1 szt.:

1) Przez serwer dyskowy Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe serwera dyskowego bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami.

2) Oferowany model serwera dyskowego musi znajdować się na liście SPC BENCHMARK 1™ (wymagane potwierdzenie w postaci raportu dostępnego pod adresem http://spcresults.org/benchmarks/results/spc1-spc1e) – oferowany model serwera dyskowego musi osiągać wydajność w teście SPC BENCHMARK 1™ minimum 200000 IOPS (SPC-1 IOPS™).

3) Serwer dyskowy musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski. Serwer dyskowy musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maksymalnie 8U w szafie.

4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia zapewniający bezprzerwową pracę serwera dyskowego bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia).

5) Możliwość dalszej rozbudowy o moduły, dodatkowe dyski i przestrzeń dyskową o zajętości w szafach przemysłowych standardu 19” nie większej niż:

a) 2U przy gęstości upakowania minimum 24 dysków 2,5”,

b) 2U przy gęstości upakowania minimum 12 dysków 3,5” lub 4U przy gęstości upakowania minimum 24 dyski 3,5”.

6) W przypadku konfiguracji serwera dyskowego z dwoma kontrolerami wszystkie zewnętrzne połączenia kablowe pomiędzy modułami muszą zapewniać komunikację nawet w przypadku awarii jednej z półek ze wszystkimi pozostałymi półkami/dyskami. Połączenia kablowe pomiędzy modułami zapewniają przepustowość minimum 48Gb/s w ramach pojedynczego połączenia.

7) Model oferowanego serwera dyskowego musi obsługiwać przestrzeń dyskową w trybie surowym (tzw. RAW) min. 2400TiB bez konieczności wymiany zainstalowanych kontrolerów i z zaoferowaną ilością kontrolerów.

8) Serwer dyskowy musi posiadać minimum 24 dysków 2,5” SAS o pojemności minimum 1800 GB każdy i prędkości obrotowej minimum 10 tysięcy obrotów na minutę.

9) Kontrolery serwera dyskowego obsługują tryb pracy w układzie active-active lub mesh-active. Serwer dyskowy będzie dostarczony z zainstalowanymi minimum 2 kontrolerami. Kontrolery serwera dyskowego wyposażone są w procesor wykonany w technologii wielordzeniowej z minimum 6 rdzeniami. Model oferowanego serwera dyskowego obsługuje min. 250 dysków wykonanych w technologii hot-plug bez konieczności wymiany lub dodawania dodatkowych kontrolerów.

10) Każdy z kontrolerów serwera dyskowego posiada po minimum 16 GB pamięci podręcznej Cache – zawartość pamięci Cache z danymi do zapisu na dyskach musi być identyczna dla wszystkich kontrolerów serwera dyskowego. Możliwość rozbudowy pamięci cache do 32 GB per kontroler.

11) Serwer dyskowy obsługuje rozbudowę pamięci podręcznej cache dla operacji odczytu do minimum 800GB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności dysków SSD.

12) Kontrolery umożliwiają ich wymianę - w przypadku awarii lub planowych zadań utrzymaniowych - bez konieczności wyłączania zasilania całego urządzenia. Wymaganie w przypadku konfiguracji z minimum 2 kontrolerami.

13) Serwer dyskowy musi posiadać dedykowane minimum 4 interfejsy RJ-45 Ethernet obsługujące połączenia z prędkością min. 100Mb/s i min. 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym serwera dyskowego.

14) Każdy kontroler serwera dyskowego pozwala na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC SAN oraz NAS. Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery serwera dyskowego wspierają min. protokoły transmisji: FC, iSCSI. Dla obsługi operacji plikowych I/O w sieci NAS Ethernet kontrolery serwera dyskowego wspierają minimum protokoły dostępu: CIFS, NFS przy czym obsługa protokołów CIFS i NFS odbywa się jednocześnie. Dla obsługi protokołów NFS i CIFS model oferowanego serwera dyskowego pozwala na instalację minimum 4 interfejsów Ethernet 10Gb lub minimum 8 portów Ethernet 1Gb/s z portami wyprowadzonymi na kontrolerach serwera dyskowego.

15) Serwer dyskowy jest wyposażony w nadmiarowe mechanizmy badania integralności składowanych danych.

16) Zamawiający wymaga, aby serwer dyskowy posiadał aktywne porty dla obsługi operacji blokowych. Oferowany serwer dyskowy musi mieć minimum 2 porty typu FC 16Gb/s, do dołączenia serwerów bezpośrednio lub do dołączenia do sieci SAN, wyprowadzone na każdy kontroler RAID. Dodatkowo należy dostarczyć min. jedna wkładkę longwave SFP+ 16G.

17) Serwer dyskowy umożliwia wymianę portów do transmisji danych na porty obsługujące co najmniej protokoły: iSCSI 10Gb/s, iSCSI 1 Gb/s oraz porty 1/10Gb Ethernet dla dostępu plikowego. 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.

18) Serwer dyskowy zapewnia poziom zabezpieczenia danych na dyskach definiowany co najmniej poziomami RAID: 0, 1 , 5 , 6.

19) Wszystkie dyski wspierane przez oferowany model serwera dyskowego wykonane są w technologii hot-plug i posiadają podwójne porty SAS obsługujące tryb pracy full-duplex.

20) Oferowany serwer dyskowy wspiera co najmniej poniższe dyski hot-plug:
- dyski elektroniczne: SSD SAS o pojemności minimum 400GB, SSD SAS SED lub FDE o pojemności minimum 800GB
- dyski mechaniczne: HDD SAS o pojemności minimum 600GB i prędkości 15 tysięcy obrotów na minutę, 300GB i prędkości 10 tysięcy obrotów na minutę, HDD NL-SAS o pojemności minimum 1TB i prędkości obrotowej minimum 7,2 tysięcy obrotów na minutę.

21) Serwer dyskowy obsługuje dyski hot-plug SSD i HDD wyposażone w porty SAS 12Gb/s zainstalowane w dowolnym module rozwiązania.

22) Model serwera dyskowego pozwala na instalację dysków hot-plug w formacie 2,5” i 3,5”.

23) Serwer dyskowy ma posiadać możliwość obsługi minimum 48 dysków SAS SSD w całym rozwiązaniu.

24) Serwer dyskowy wspiera mieszaną konfigurację dysków typu SAS, NearLine-SAS i SSD w obrębie każdego pojedynczego modułu obudowy pozwalającego na instalacje dysków hot-plug.

25) 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.

26) Serwer dyskowy objęty jest minimum 36 miesięcznym okresem gwarancji z gwarantowanym czasem naprawy w ciągu 24h od zgłoszenia usterki w miejscu instalacji urządzenia. Zgłaszanie skuteczne usterek w trybie całodobowym, tj. 7 dni w tygodniu, również w dni świąteczne. Zgłoszenia usterek muszą być akceptowane zarówno drogą email, jak również drogą telefoniczną (kontakt w języku polskim, nie dopuszcza się numerów o podwyższonej płatności). Linia telefoniczna musi być czynna 24 godziny na dobę tj. 7 dni w tygodniu również w dni świąteczne. W razie awarii dyski pozostają u Zamawiającego.

27) Serwis gwarancyjny obejmuje dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia przez cały okres obowiązywania gwarancji.

28) System zapewnia możliwość samodzielnego i automatycznego powiadamiania o usterkach za pomocą wiadomości wysyłanych poprzez protokół SNMP (wersja: 1 ,2c, 3) lub SMTP.
29) System musi mieć możliwość objęcia go proaktywnym serwisem rozumianym jako zdalna prewencyjna diagnostyka sprzętu z możliwością automatycznego zakładania zgłoszenia w systemie serwisowym bez ingerencji administratora.
30) Sprzęt fabrycznie nowy. Nie dopuszcza się użycia serwerów dyskowych odnawianych, demonstracyjnych lub powystawowych.
31) Urządzenie wykonane jest zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia.
32) Oprogramowanie do zarządzania zintegrowane jest z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI) jak i do obsługi transmisji protokołami CIFS oraz NFS. Komunikacja z wbudowanym oprogramowaniem zarządzającym serwerem dyskowym odbywa się w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym a zdalne zarządzanie serwerem dyskowym odbywa się bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.
33) Serwer dyskowy wyposażony 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 oferowanego serwera dyskowego.
34) Serwer dyskowy umożliwia zdefiniowanie minimum 4096 woluminów tzw. LUN.
35) Serwer dyskowy umożliwia aktualizację oprogramowania wewnętrznego, kontrolerów RAID i dysków bez konieczności wyłączania serwera dyskowego i bez konieczności wyłączania ścieżek logicznych iSCSI dla podłączonych serwerów.
36) Serwer dyskowy umożliwia dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w serwerze dyskowym) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupę dyskową.
37) Serwer dyskowy posiada wsparcie dla systemów operacyjnych: MS Windows Server 2012 R2/2016, Oracle Linux 7, RedHat Ent Linux 7, Solaris 10/11, VMWare 6.0/6.5 , Citrix XEN Server 7.
38) Serwer dyskowy będzie dostarczony z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) dla połączeń FC i iSCSI.
39) Serwer dyskowy obsługuje woluminy logiczne o maksymalnej pojemności minimum 16TB.
40) Serwer dyskowy posiada możliwość uruchomienie mechanizmów zdalnej replikacji danych - w trybie synchronicznym i asynchronicznym - po protokołach FC oraz iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji.
Powyższa funkcjonalność nie jest objęta w postępowaniu lecz będzie umożliwiała Zamawiającemu rozbudowę w przyszłości systemu pamięci masowych.
41) Serwer dyskowy posiada możliwość obsługi deduplikacji i kompresji danych na dyskach wbudowanych w serwer dyskowy (nie dopuszcza się główek, kompresji zewnętrznej, programowej itp.) w następujących trybach równocześnie: sama deduplikacja, sama kompresja, deduplikacja i kompresja oraz niezależnie na poziomie każdego LUN.
Powyższa funkcjonalność nie jest objęta w postępowaniu lecz będzie umożliwiała Zamawiającemu rozbudowę w przyszłości systemu pamięci masowych.
42) Funkcjonalność replikacji danych jest zapewniona z poziomu oprogramowania wewnętrznego serwera dyskowego.
43) Serwer dyskowy obsługuje QoS (ang. Quality of Services) czyli nadawanie priorytetów obsługi transmisji I/O dla skonfigurowanych hostów, LUN-ów, portów do hostów. Jeżeli funkcjonalność ta wymaga odrębnej licencji należy dostarczyć ją wraz z serwerem dyskowym dla zaoferowanej pojemności serwera dyskowego.
44) Wraz z serwerem dyskowym należy zapewnić wsparcie dla mechanizmów Offloaded Data Transfer i Space Reclamation.
45) Serwer dyskowy obsługuje mechanizmy Thin Provisioning czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w serwerze dyskowym. Jeżeli taka funkcjonalność wymaga dodatkowych licencji to należy je dostarczyć wraz z serwerem dyskowym dla maksymalnej pojemności dyskowej oferowanego serwera

dyskowego. Model oferowanego serwera dyskowego musi wspierać rozwiązania klasy „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów dyskowych serwera dyskowego dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 serwerami dyskowymi. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do serwera dyskowego (serwer dyskowy podstawowy) w przypadku wystąpienia awarii logicznego połączenia z tym serwerem dyskowym bądź awarii samego serwera dyskowego, powodujących dla danego środowiska brak dostępu do zasobów serwera dyskowego podstawowego. Powyższa funkcjonalność nie jest objęta w postępowaniu lecz będzie umożliwiała Zamawiającemu rozbudowę w przyszłości systemu pamięci masowych.

46) Replikacja danych pomiędzy serwerami dyskowymi podstawowym i zapasowym, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać poziomy co najmniej RAID1, RAID10, RAID5, RAID6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy serwerami dyskowymi podstawowym i głównym.

47) Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii serwera dyskowego podstawowego (tzw. automated failover).

48) Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z serwera dyskowego podstawowego na zapasowy (tzw. manual failover).

49) Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z serwera zapasowego na podstawowy po usunięciu awarii serwera dyskowego podstawowego (tzw. failback).

50) Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z serwera zapasowego zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.

51) Funkcjonalność „wysokiej dostępności” musi wspierać dwukierunkowe przełączanie serwera dyskowego podstawowego na zapasowy.

52) Oświadczenie Wykonawcy, iż serwery dyskowe mają jednolitą platformę sprzętową.

1.2. Przełącznik sieciowy sieci SAN o następujących parametrach minimalnych – 2 szt.:

1) Ilość portów FC o następujących wymaganiach minimalnych:
Ilość aktywnych portów FC min. 16 w tym każdy min. 32gbit/s. Rozbudowa nie może odbywać się poprzez zakupu dodatkowych (z wyłączeniem modułów SFP/SFP+ lub kabli, modułów sprzętowych) jedynie poprzez zakup licencji. W pełni rozbudowany przełącznik nie może zajmować w szafie RACK więcej niż 1U.

2) Przepustowość portu o następujących wymaganiach minimalnych:
Porty uniwersalne o przepustowości min. 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 o następujących wymaganiach minimalnych:
Moduły do transmisji światłowodowej z prędkością min. 16Gb/s poprzez kabel światłowodowy wielomodowy z interfejsem LC w ilości min. 14 sztuk oraz min. 1 moduł światłowodowy z prędkością min. 16Gb/s poprzez kabel światłowodowy jednomodowy.

4) Inne funkcje i wyposażenie o następujących wymaganiach minimalnych:

a) Możliwość obsługi min. trybów pracy portów FC: D_Port, E_port, F_port, N-Port.

b) Możliwość obsługa funkcji PoD przydziału licencji dla aktywnych portów FC.

c) Aktywne licencje:

- min. Webtools,
- min. FullFabric (z obsługą do min. 239 przełącznzików FC),
- min. Zoning,
- min. Ports on Demand.

d) Możliwość zdalnej aktualizacji firmware'u switcha.

e) Możliwość obsługi funkcjonalności:

- min. FabricWatch, Trunking, Adaptive Networking, Access Gateway,
- min. Advanced Performance Monitoring,
- min. Inter Switch Link (ISL) z przepustowością maks. 256 Gb/s /ISL.

f) Dedykowany interfejs RJ-45 min 10/100/1000 Mb/s do zarządzania poprzez sieć Ethernet.
g) Możliwość zarzadzania typu in-band poprzez FC.
h) Dedykowany interfejs RJ-45 lub DB9 do zarządzania poprzez interfejs szeregowy, dedykowany port USB umożliwiający upgrade FW i zapis logów.
i) Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia.
j) Możliwość zarządzania poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych min. 128-bit SSL oraz poprzez usługę SSH.
k) Możliwość zarządzania poprzez konsole znakową tzw. CLI.
l) Wsparcie dla protokołu min. SNMP v.3.

5) Typ obudowy o następujących wymaganiach minimalnych:
a) Montowany w szafie typu rack 19”. Wysokość przełącznika max. 1U w systemie montażu w szafie typu rack 19”. Wraz ze switchem należy dostarczy wszystkie niezbędne do uruchomienia kable połączeniowe o odpowiedniej długości.

6) Gwarancja/dostawa:
Urządzenie musi być objęte gwarancją na okres min. 36 miesięcy z gwarantowanym czasem naprawy w miejscu instalacji urządzenia najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

1.3. Przełącznik sieciowy sieci LAN o następujących parametrach minimalnych – 2 szt.:

1) Ilość portów o następujących parametrach minimalnych:
a) Urządzenie musi umożliwiać obsadzenie minimum 48 portami min. 1GE/10GE definiowanych za pomocą wkładek SFP/SFP+,
b) Urządzenie musi zapewniać min. 6 portów min. 40G QSFP+,
c) Wszystkie porty 1GE/10GE/40GE muszą być aktywne,
d) Urządzenie musi obsługiwać wkładki typu 1GE RJ45, 1GE-SX, 10GE-SR oraz 10GE-LR,
e) Urządzenie musi obsługiwać kable typu 10GE Twinax.

2) Parametry wydajnościowe:
a) Wymagana jest prędkość przełączania „wirespeed” dla każdego portu,
b) Wymagana jest przepustowość przełączania 720 Gbps (1440 Gbps duplex),
c) Wymagany rozmiar tablicy MAC to min. 288000.

3) Wymiary:
a) Obudowa musi być przeznaczona do montażu w szafie rackowej 19”,
b) Wysokość urządzenia maksymalnie 1U.

4) Implementacja zaleceń IEEE:
Urządzenie musi obsługiwać następujące protokoły:
a) min. IEEE 802.1ab LLDP,
b) min. IEEE 802.1p Class of Service,
c) min. IEEE 802.1d Spanning Tree Protocol,
d) min. IEEE 802.1Qau Congestion Notification,
e) min. IEEE 802.1Qaz Enhanced Transmission Selection (ETS),
f) min. IEEE 802.1Qbb Priority Flow Control (PFC),
g) min. IEEE 802.1q VLAN,
h) min. IEEE 802.1s Multiple Spanning Tree Protocol,
i) min. IEEE 802.1w Rapid Spanning Tree Protocol,
j) min. IEEE 802.1x Port Based Network Access Control,
k) min. IEEE 802.3ad LACP,
l) min. IEEE 802.3x Flow Control.

5) Link agregation:
Urządzenie musi zapewniać zgodność:
a) min. static LAG oraz LACP,

b) min. obsługa 48 portów w LAG,
c) min. dla technologii virtual port channel (VPC).
6) Mechanizmy Data Center oraz wirtualizacji:
Urządzenie musi zapewniać zgodność:
a) min. dla Data Center Bridging (DCB),
b) min. dla FIP snooping,
c) min. dla Edge Virtual Bridging (EVB),
d) min. obsługa DCVPN gateway (VXLAN, VTEP, NVE).
7) Urządzenie musi zapewniać zgodność:
a) min. port konsoli CLI,
b) min. port RJ45 10/100/1000Mbps do zarządzania urządzeniem,
c) min. port USB,
d) min. dla SSHv2,
e) min. dla NETCONF oraz OVSDB,
f) min. dla protokołów Authentication, authorization, and accounting (AAA),
g) min. dla RADIUS,
h) min. dla SNMP v2c, v3,
i) min. dla Remote monitoring (RMON).
8) Zasilanie:
Oferowane urządzenia muszą być wyposażone w min. 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.
9) Moduły SFP oraz SFP+:
a) Należy dostarczyć min. 12 modułów SFP+ 10Gb SR (MM),
b) Należy dostarczyć min. 2 moduły SFP+ 10Gb LR (SM).
c) Wszystkie moduły SFP/SFP+/QSFP+ muszą znajdować się na liście kompatybilności zaoferowanego urządzenia oraz pochodzić z oficjalnego kanału sprzedaży.
10) Tryb pracy:
a) Urządzenie musi posiadać możliwość pracy w trybie tzw. End Host Mode, w którym:
- Do minimum ograniczono konfiguracyjny nakład pracy potrzebny do dołączenia urządzenia do istniejącej sieci LAN,
- Wyeliminowano ingerencję w istniejącą domenę STP (Spanning Tree Protocol) oraz możliwość wystąpienia pętli (zablokowana komunikacja między portami uplink),
- Porty grupuje się w instancje, między którymi dozwolona jest komunikacja, komunikacja między instancjami nie jest dozwolona.

b) Urządzenie musi posiadać możliwość zdalnej konfiguracji/monitoringu przez dedykowane oprogramowanie
c) Urządzenie musi zapewniać możliwość przekazania informacji o stanie portu/grupy portów typu uplink do portów typy downlink z jednoczesnym uzależnieniem stanu portu typu downlink od stanu portu typu uplink
11) Gwarancja:
Urządzenie musi być objęte gwarancją na okres min. 36 miesięcy z gwarantowanym czasem naprawy w miejscu instalacji urządzenia najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

1.4. Serwer zarządzający o następujących parametrach minimalnych – 1 szt. :

1) Obudowa o następujących parametrach minimalnych:
a) Typu Rack, wysokość maksimum 1U;
b) Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy.
2) Płyta główna o następujących parametrach minimalnych:
a) co najmniej dwuprocesorowa, umożliwiająca instalację procesorów min. dwunastordzeniowych,
b) wyposażona w min. 24 gniazda pamięci RAM DDR4, z możliwością obsługi min. 3000GB pamięci RAM DDR4 min. 2966 Mhz;
c) Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 1000GB (przez pamięć nieulotną rozumie się moduły pamięci

zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci),

d) Min. 3 złącza PCI Express generacji min. 3 o prędkości x16 (nie wliczając ewentualnego złącza dedykowanego dla kontrolera RAID),
e) Wszystkie złącza PCI Express muszą być aktywne,
f) Min. 2 sloty dla dysków w slocie typu 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 typu M.2 bez zajmowania klatek dyskowych serwera),
g) Zainstalowane dwie karty microSD o pojemności min 64GB z możliwością konfiguracji w RAID1.

3) Procesory o następujących parametrach minimalnych:
a) Zainstalowane min. dwa procesory min. 12-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECrate2017_int_base minimum 131 pkt. dla dowolnej platformy dwuprocesorowej serwera, który jest dostępny na stronie spec.org,

4) Pamięć RAM o następujących parametrach minimalnych:
a) Zainstalowane min. 32 GB pamięci RAM typu DDR4 Registered, co najmniej 2966Mhz w kościach o pojemności min. 16GB,
b) Możliwość wsparcia dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC,
c) Możliwość wsparcia dla konfiguracji pamięci w trybie „Rank Sparing”,

5) Kontrolery dyskowe, I/O o następujących parametrach minimalnych:
a) Zainstalowany kontroler typu co najmniej SAS 3.0 RAID 0,1,5,6,50,60 1GB pamięci podręcznej cache,
b) Wyposażony w nieulotną pamięć cache.

6) Dyski twarde o następujących parametrach minimalnych:
a) Brak dysków twardych,
b) Minimum 8 wnęk dla dysków twardych Hotplug 2,5.

7) Kontrolery LAN o następujących parametrach minimalnych:
a) Min. jedna dwuportowa karta z min. 2x1Gbit/s z możliwością wsparcia iSCSI, niezajmująca slotu PCI Express,
b) Dodatkowa osobna karta min. 4x10Gbit/s SFP+ wraz z wkładkami SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express).

8) Kontrolery I/O FC/SAS/Inne o następujących parametrach minimalnych:
a) Jedna dwuportowa karta np. typu FC 16GB chipset QLE2692;

9) Porty o następujących parametrach minimalnych:
a) zintegrowana karta graficzna ze złączem VGA,
b) min. 2x USB 3.0 dostępne na froncie obudowy,
c) min. 2x USB 3.0 dostępne z tyłu serwera,
d) min. 1x USB 3.0 wewnątrz serwera,
e) 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.

10) Zasilanie, chłodzenie o następujących parametrach minimalnych:
a) Redundantne zasilacze hotplug o mocy min. 450W, o sprawności min. 94% (tzw klasa Platinum),
b) Redundantne wentylatory hotplug.

11) Zarządzanie o następujących parametrach minimalnych:
a) Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera,
b) zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,

- Dedykowana karta LAN min. 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,
- Możliwość dostępu poprzez przeglądarkę Web (także SSL, SSH),
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii,
- Zarządzanie alarmami (zdarzenia poprzez SNMP),
- Możliwość przejęcia konsoli tekstowej,
- Możliwość przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),
- Możliwość sprzętowego monitoringu 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 – możliwość wirtualizacji MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 8Gbit/s),
- Oprogramowanie zarządzające i diagnostyczne 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 serwisu o zaistniałej lub zbliżającej się usterce.

12) Zgodność z systemami operacyjnymi min. Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL.

13) Dokumentacja, inne:

a) Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego.

b) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www;

14) Gwarancja:

a) min. 36 miesięcy gwarancji w trybie on-site z gwarantowanym czasem skutecznej naprawy w ciągu 24h od zgłoszenia usterki,

b) Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dla oferowanego serwera.

1.5. Serwer produkcyjny o minimalnych parametrach – 6 szt.:

1) Obudowa o następujących parametrach minimalnych:

a) Typu Rack, wysokość maksimum 1U;
b) Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy;
2) Płyta główna o następujących parametrach minimalnych:
a) min. dwuprocesorowa umożliwiająca instalację procesorów dwunastordzeniowych,
b) wyposażona w min. 24 gniazda pamięci RAM DDR4, z możliwością obsługi min. 3000GB pamięci RAM DDR4 2966 Mhz,
c) Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 1000GB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci),
d) Minimum 3 złącza PCI Express generacji min. 3 o prędkości x16 (nie wliczając ewentualnego złącza dedykowanego dla kontrolera RAID,
e) Wszystkie złącza PCI Express muszą być aktywne,
f) Minimum 2 sloty dla dysków typu 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 typu M.2 bez zajmowania klatek dyskowych serwera),
g) Zainstalowane co najmniej dwie karty microSD o pojemności min 64GB z możliwością konfiguracji w RAID1.
3) Procesory o następujących parametrach minimalnych:
a) Zainstalowane minimum dwa procesory min. 12-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECrate2017_int_base minimum 131 pkt. dla dowolnej platformy dwuprocesorowej dostępnego na stronie spec.org.
4) Pamięć RAM o następujących parametrach minimalnych:
a) Zainstalowane min. 256 GB pamięci RAM typu DDR4 Registered, min. 2966Mhz w kościach o pojemności min. 32GB;
b) Możliwość wsparcia dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC,
c) Możliwość wsparcia dla konfiguracji pamięci w trybie „Rank Sparing”,
5) Kontrolery dyskowe, I/O o następujących parametrach minimalnych:
a) Zainstalowany kontroler typu SAS 3.0 co najmniej RAID 0,1,5,6,50,60 1GB pamięci podręcznej cache,
b) Wyposażony w nieulotną pamięć cache;
6) Dyski twarde o następujących parametrach minimalnych:
a) Brak dysków twardych;
b) Min. 8 wnęk dla dysków twardych Hotplug 2,5;
7) Kontrolery LAN o następujących parametrach minimalnych:
a) Min. jedna dwuportowa karta min. 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express,
b) Dodatkowa osobna karta min. 4x10Gbit/s SFP+ wraz z wkładkami SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express)
8) Kontrolery I/O FC/SAS/Inne o następujących parametrach minimalnych:
a) Min. Jedna dwuportowa karta typu FC 16GB;
9) Porty o następujących parametrach minimalnych:
a) zintegrowana karta graficzna ze złączem VGA,
b) min. 2x USB 3.0 dostępne na froncie obudowy,
c) min. 2x USB 3.0 dostępne z tyłu serwera,
d) min. 1x USB 3.0 wewnątrz serwera,
e) 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.
10) Zasilanie, chłodzenie o następujących parametrach minimalnych:
a) Redundantne zasilacze hotplug o mocy min. 450W, o sprawności co najmniej 94% (tzw klasa Platinum),
b) Redundantne wentylatory hotplug.
11) Zarządzanie o następujących parametrach minimalnych:
a) Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express,

procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera,

b) Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera,
- Dedykowana karta LAN min. 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,
- Możliwość dostępu poprzez przeglądarkę Web (także SSL, SSH),
- Możliwość zarządzania mocą i jej zużyciem oraz monitoring zużycia energii,
- Możliwość zarządzania alarmami (zdarzenia poprzez SNMP),
- Możliwość przejęcia konsoli tekstowej,
- Możliwość przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM),
- Możliwość sprzętowego monitoringu 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 – możliwość wirtualizacji MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 8Gbit/s),
- Oprogramowanie zarządzające i diagnostyczne 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 serwisu o zaistniałej lub zbliżającej się usterce.

12) Zgodność z systemami operacyjnymi min. Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL

13) Dokumentacja, inne:

a) Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego,

b) Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www;

14) Gwarancja:
a) min. 36 miesięcy gwarancji w trybie on-site z gwarantowanym czasem skutecznej naprawy w ciągu 24h od zgłoszenia usterki,
b) Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dla oferowanego serwera.

1.6. Dostawa, instalacja, konfiguracja oraz uruchomienie:

1) Powyższe urządzenia należy zainstalować i skonfigurować w dostarczonej szafie przemysłowej standardu 19” wyposażonej w listwy zasilające, organizatory okablowania, kable komunikacyjne, elementy monitoringu środowiskowego współpracującego z Systemem monitoringu środowiskowego opisanego w pozycji „Oprogramowanie i wyposażenie serwerowni Uniwersyteckiego Centrum Informatyzacji – oprogramowanie”, zapewniające odpowiednie warunki pracy urządzeń.
2) Usługa instalacji, konfiguracji i uruchomienia urządzeń będących przedmiotem dostawy:
a) Przed przystąpieniem do prac należy przygotować do akceptacji Zamawiającego koncepcję techniczną instalacji i harmonogram prac w zakresie dostarczanej infrastruktury.
b) Opracowanie dokumentacji powykonawczej i zaleceń powdrożeniowych obejmujące:
- Szczegółowy opis konfiguracji urządzeń.
- Szczegółowy schemat połączeń pomiędzy urządzeniami (w formie graficznej i opisowej).
- Procedury operacyjne dla administratorów.

3) Dostarczane w ramach realizacji dokumenty, opracowania i inne materiały muszą zawierać co najmniej:
a) Koncepcję techniczną i harmonogramu prac zawierających minimalnie:
- Zestawienie dostarczonych elementów sprzętowych,
- Rysunki logiczne rozwiązania,
- Rysunki połączeń fizycznych ze wskazaniem odpowiednich portów w odpowiednich urządzeniach,
- Oznaczenia połączeń fizycznych,
- Zestawienie wymaganych wersji oprogramowania podstawowego i rozszerzeń (o ile ma to zastosowanie),
- Zestawienie wymaganych łat systemu operacyjnego (ang. Patch Management),

b) Opis testów zawierający minimalnie:
- Zestawienie stosowanej nomenklatury,
- Weryfikację zgodności konfiguracji z koncepcją techniczną (o ile ma to zastosowanie),
- Weryfikację odporności na awarie pojedynczych komponentów sprzętowych,
- Wyniki testów należy podać w postaci tabelarycznej.

4) Dokumentacja powykonawcza i zalecenia powdrożeniowe zawierający minimalnie:
a) Zestawienie stosowanej nomenklatury,
b) Rysunki logiczne rozwiązania,
c) Zestawienie nazewnictwa poszczególnych elementów systemu,
d) Rysunki połączeń fizycznych ze wskazaniem odpowiednich portów w odpowiednich urządzeniach,
e) Zestawienie oznaczeń połączeń fizycznych,
f) Zestawienie zainstalowanych wersji oprogramowania podstawowego i rozszerzeń (o ile ma to zastosowanie),
g) Weryfikację zgodności przyjętych oznaczeń połączeń fizycznych z koncepcją techniczną.
5) Instruktaż z dostarczonej infrastruktury serwerowo – sieciowej:
a) przedstawienie i omówienie funkcjonalności, parametrów, konfiguracji dostarczonej infrastruktury (serwery, serwery dyskowe, switche sieci SAN i LAN),
b) omówienie wykonanej konfiguracji połączeń,
c) przedstawienie i omówienie funkcjonalności dostarczonych elementów systemu wirtualizacji,
d) omówienie wykonanej konfiguracji systemu monitoringu środowiskowego
e) przedstawienie i omówienie funkcjonalności dostarczonych elementów zasilania awaryjnego,
f) przedstawienie i omówienie funkcjonalności dostarczonych elementów systemu backupu.
6) Instruktaż z zarządzania i ochrony danych oferowanej infrastruktury (serwery, serwery dyskowe, switche sieci SAN i LAN 10Gb).
7) Szczegółowe prace instalacyjno-konfiguracyjne:

a) Przed przystąpieniem do instalowania dostarczonej infrastruktury sprzętowej Wykonawca zobowiązany jest:
- dostarczone urządzenia uruchomić a następnie podłączyć do istniejącej infrastruktury,
- zrekonfigurować środowisko sieci LAN, SAN dla wszystkich urządzeń objętych procesem wdrożenia (switche, serwery, serwery dyskowe),
- dostarczyć, jeżeli będzie to konieczne wszystkie wymagane licencje i moduły w celu poprawnego uruchomienia infrastruktury informatycznej,
- zaktualizować wersję oprogramowania na przełącznikach sieci LAN, SAN.

b) Nowo dostarczane środowisko sprzętowe należy zamontować w szafie. Zasilanie musi być połączone redundantnie dla każdego z nowo instalowanych elementów. W przypadku urządzeń nie mających redundantnych zasilaczy należy je podłączyć poprzez urządzenie umożliwiające bezprzerwowe przełączenie z dwóch źródeł zasilania.

c) Nowo instalowane środowisko należy przed uruchomieniem produkcyjnym zaktualizować w oparciu o weryfikacje na listach HCL.

8) Roboty instalacyjne.

W związku z rozbudową środowiska informatycznego i zmianą warunków środowiskowych oraz technicznych serwerowni konieczna jest modernizacja infrastruktury technicznej serwerowni, obejmująca:

a) Reorganizacje rozmieszczenia.
- W związku z doposażeniem serwerowni w nowe urządzenia należy zreorganizować rozłożenie urządzeń w pomieszczeniu tak aby efektywnie wykorzystać przestrzeń pomieszczenia.
- W przypadku konieczności reorganizacji ustawienia istniejących szaf w pomieszczeniu serwerowni, pozycję szaf, sposób ich przesunięcia należy ustalić z Zamawiającym.

b) Instalację nowej szafy serwerowej z wyposażeniem
- Na potrzeby nowo instalowanych urządzeń informatycznych należy dostarczyć i zainstalować szafę serwerową z akcesoriami.
- Zamawiający wymaga udzielenia gwarancji na prace instalacyjno-modernizacyjno-konfiguracyjne min. 36 miesięcy.
- Zamawiający nie dopuszcza realizacji przedmiotu zamówienia zdalnie. Wszelkie prace instalacyjno – konfiguracyjne musza odbyć się w uzgodnionych z Zamawiającym terminach poza godzinami pracy uczelni.

1.7. Zasilanie awaryjne

1) W celu podłączenia nowo dostarczanych zasilaczy awaryjnych należy przygotować infrastrukturę elektryczną serwerowni do podłączenia oferowanego sprzętu serwerowego w zakresie:

a) modernizacji rozdzielni elektrycznych,
b) przygotowania nowych obwodów równoległych,
c) przygotowania tras kablowych,
d) przygotowania instalacji elektrycznej dla przyłącza agregatu w rozdzielni elektrycznej budynku,
e) dostarczenia zasilaczy typu UPS (min. dwa zasilacze UPS dla zapewnienia redundancji zasilania równoległego, 3f/f, moduły bateryjne, zewnętrzne bypass, autonomia każdego z zasilaczy ok. 30 min).

2) Gwarancja min. 36 miesięcy.

1.7.1. Elektryczno-logiczna infrastruktura przyłączeniowa

1) Na potrzeby zasilania nowej szafy serwerowej należy zmodernizować istniejącą instalację zasilania szaf serwerowych.
- W ramach modernizacji należy wykonać instalację zasilania awaryjnego rozdzielni z agregatu z ręcznym przełączeniem zasilania agregat – sieć.
- Gniazdo przyłączeniowe agregatu należy zainstalować na elewacji budynku (obok wejścia do budynku z pomieszczeniem klastra obliczeniowego) w zamykanej na klucz obudowie, a okablowanie doprowadzić do przełącznika sieć-agregat, który należy zainstalować w pomieszczeniu klastra.
- Z przełącznika należy zasilić rozdzielnię.

2) Drugim elementem modernizacji jest rozbudowa rozdzielni.

- Z rozdzielni należy wyprowadzić dwa nowe obwody trójfazowe min. 32A na potrzeby zasilania nowo instalowanych zasilaczy UPS.
- Przewody obwodów należy zakończyć gniazdami montowanymi na podwieszanej trasie kablowej (analogicznie jak istniejące). Zasilacze należy podłączać za pomocą odpowiednich wtyków do tych gniazd.
- W celu doprowadzenia okablowania zasilającego i logicznego do nowej szafy należy rozbudować istniejąca trasę kablową nad szafami tak, aby umożliwić doprowadzenie okablowania do nowej szafy serwerowej oraz montaż gniazd zasilających UPS.
- Wraz z szafą należy dostarczyć całość okablowania potrzebnego do połączenia wszystkich urządzań montowanych w szafie.

1.7.2. Szafa serwerowa RACK 19" wraz z wyposażeniem o minimalnych parametrach – 1 szt.:

1) Konstrukcja i minimalne wymagania instalacyjne:
a) Możliwość wykorzystania 42U pojemności użytecznej do instalacji urządzeń w pozycji poziomej.
b) Wymiary instalacyjne (tzw. footprint) szafy w serwerowni:
- całkowita wysokość maksymalna 2000mm,
- całkowita głębokość maksymalna 1200mm,
- całkowita szerokość maksymalna 600mm.

2) Szafa musi zapewniać możliwość demontażu wszystkich głównych wsporników pionowych.
3) Klasa ochrony co najmniej IP20.
4) Szafa musi być wyposażona w:
a) przednie drzwi perforowane, zamykane na zamek z kluczem, jednoskrzydłowe, możliwość montażu przednich drzwi lewa/prawa strona, poziom perforacji minimum 80%,\
b) tylne drzwi perforowane, dwuskrzydłowe dla ograniczenia przestrzeni serwisowej, zamykane na zamek z kluczem wspólny z zamkiem przednim,
c) zdejmowane panele boczne zabezpieczone zamkiem,
d) stopki zintegrowane z kółkami dla możliwości łatwego przemieszczania całej szafy po powierzchniach płaskich,

5) Szafa musi zapewniać chłodzenie horyzontalne przód-tył, pasywne – bez wentylatorów wspomagających.
6) Szafa musi posiadać fabryczne zabezpieczenie przeciwko wywróceniu szafy do przodu (tzw. anti-tilt protection), montaż tego zabezpieczenia musi być możliwy bez konieczności wyłączania urządzeń zamontowanych w szafie.
7) Przestrzeń instalacyjna bez zainstalowanych urządzeń musi być wyposażona w zaślepki montowane beznarzędziowo od frontu szafy.
8) Udźwig gwarantowany szafy musi wynosić co najmniej 1000 kg dla instalowanych urządzeń, w warunkach dynamicznych (tj. z możliwością przemieszczania szafy z zainstalowanym sprzętem o wskazanej wadze).
9) Szafa musi być przystosowana do poprawnej instalacji dostarczonych serwerów i macierzy wraz z ich fabrycznymi prowadnicami przewodów.
10) Szafa musi pozwalać na trwałe łączenie wielu szaf jednakowego typu.
11) Szafa musi zapewniać pełną kompatybilność w zakresie montażu urządzeń różnych producentów dedykowanych do instalacji w szafach przemysłowych 19” rack zgodnych z normami: EIA310-D, DIN41494 i IEC 297.
12) Szafa musi zawierać całość okablowania niezbędnego do realizacji połączeń logicznych oraz do realizacji dystrybucji zasilania – okablowanie musi posiadać widoczne oznakowanie na złączach wykorzystanych dla fizycznych połączeń pomiędzy zainstalowanymi urządzeniami.
13) Elementy konstrukcyjne szafy muszą posiadać minimalne zabezpieczenie antykorozyjne pokryw bocznych poprzez użycie blach ocynkowanych oraz lakierowania proszkowe dla tych elementów.
14) Dystrybucja zasilania:
a) Szafa musi posiadać zainstalowane urządzenia pomocnicze dla dystrybucji zasilania (tj. listwy PDU, kable zasilające, prowadnice do kabli) dla wszystkich urządzeń wymaganych w niniejszym postępowaniu.
b) Szafa musi umożliwiać minimum 1-torową dystrybucję zasilania jednofazowego 230V AC dla zainstalowanych urządzeń.

c) Szafa musi spełniać wymogi bezpieczeństwa eksploatacji i obsługi (certyfikat CB) oraz być wykonana zgodnie z dyrektywą RoHS w zakresie ograniczonej szkodliwość użytych materiałów i komponentów.

15) Dystrybucja zasilania dla pozostałych urządzeń:

a) Szafa musi posiadać możliwość późniejszej modyfikacji układu zasilania z wariantu zasilania jednofazowego na trójfazowe 3x380VAC 50/60Hz.

b) Należy dostarczyć min. 2 x PDU basic 16A IEC320 24x10A, UPS,cascade.

c) Szafa musi posiadać oznaczony punkt montażowy (zacisk lub śruba) dla doprowadzenia okablowanie ochronnego (uziemienie)

16) Gwarancja:
Szafa musi być objęta minimum 36-miesięczną gwarancją, która musi obejmować także akcesoria i urządzenia pomocnicze zapewniające dystrybucję zasilania dla zainstalowanych urządzeń.

W szafie serwerowej należy zamontować przełącznik o następujących parametrach minimalnych – 2 szt.:

1) Ilość portów o następujących parametrach minimalnych:

a) Min. 24 porty 10/100/1000BaseT,

b) Min. 4 porty 10Gb SFP+ min. dwa obsadzone wkładkami działającymi w standardzie 10GBaseSR.

2) Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT.

3) Wydajność przełączania co najmniej min. 128 Gbps oraz przepustowość min. 95 Mpps.

4) Obsługa min. 4094 tagów IEEE 802.1Q oraz min. 512 jednoczesnych sieci VLAN.

5) Obsługa protokołu IEEE 802.1v.

6) Funkcja automatycznego provisioningu i konfiguracji przełącznika przy jego pierwszym podłączeniu do sieci bez konieczności wykonywania wstępnej, ręcznej konfiguracji.

7) Zgodność z Energy-efficient Ethernet (EEE) IEEE 802.3az.

8) Bufor pakietów nie mniejszy niż 12MB.

9) Minimum 4GB pamięci typu Flash.

10) Minimum 1GB pamięci operacyjnej typu RAM.

11) Możliwość obsługi min. protokołów rutingu: ruting statyczny (wraz w ECMP), RIP v1, RIP v2.

12) Wielkość tablicy rutingu: minimum 2000 wpisów IPv4 i 1000 wpisów IPv6.

13) Dostęp do urządzenia przez konsolę szeregową (linia komend umożliwiająca pełne zarządzanie przełącznikiem), HTTPS, SSHv2 i SNMPv3.

14) Możliwość obsługi min. protokołów Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s).

15) Możliwość obsługi min. protokołów GVRP i MVRP.

16) Możliwość obsługi min. Secure FTP.

17) Możliwość obsługi min. 802.3ad Link Aggregation Protocol (LACP).

18) Możliwość obsługi min. Simple Network Time Protocol (SNTP) v4.

19) Wielkość tablicy adresów MAC: minimum 16000.

20) Możliwość obsługi min. LLDP i LLDP-MED.

21) Wbudowany serwer min. DHCP.

22) Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting.

23) Funkcja autoryzacji użytkowników zgodna z 802.1x .

24) Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+.

25) Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection).

26) Ochrona serwerów DHCP.

27) Możliwość obsługi min. list kontroli dostępu (ACL).

28) Możliwość obsługi min. ramek Jumbo o wielkości co najmniej 9220 bajtów.

29) Możliwość obsługi min. IP SLA dla ruchu typu VoIP (co najmniej monitoring jakości połączeń głosowych przy pomocy testów jitter UDP).

30) Obudowa wieżowa 1U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 25 cm.

31) Maksymalny pobór mocy nie większy niż 30W.

32) Minimalny zakres pracy od 0°C do 45°C.

33) Przełącznik musi być w pełni wspierany przez oprogramowanie zarządzające opisane w punkcie System zarządzania środowiskiem sieciowym.

34) Gwarancja:
Min. 36 miesięcy obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory), zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (na koszt Wykonawcy). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5.

1.7.3. Rozbudowa zasilania awaryjnego

1) W celu zapewnienia zasilania bezprzerwowego dla urządzeń IT wymaga się zastosowania systemu zasilaczy UPS składającego się z min. dwóch zestawów zasilaczy o mocy min. 6kVA każdy. Zasilacze będą pracowały w układzie redundantnym, to znaczy każde urządzenie z co najmniej dwoma zasilaczami będzie zasilone z każdego z UPS. Na potrzeby zasilenia urządzeń jedno-zasilaczowych należy zastosować przełącznik ATS. Przełącznik ten także należy zasilić z obu zasilaczy UPS. Zasilacze należy dobrać tak aby zapewniały, przy 100% obciążenia, prace autonomiczną nie krócej niż przez 30 minut. Zespół zasilaczy należy zainstalować w nowej szafie IT. W celu optymalnego obciążenia instalacji elektrycznej i zastosowanych urządzeń IT należy zastosować zasilacze typu 3F/1F. Każdy zasilaczy powinien być wyposażony w interfejs Ethernet umożliwiający zdalną konfigurację i monitoring.

2) Minimalne parametry techniczne, którymi będzie charakteryzować się pojedynczy zasilacz UPS oraz przełącznik ATS:

a) **Zasilacz awaryjny – 2 szt. :**

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań minimalnych
1	Moc pozorna	Min. 6000 VA
2	Moc rzeczywista	Min. 5400 W
3	Topologia (klasyfikacja IEC 62040-3)	On-line z korekcją współczynnika mocy
4	Sprawność przy pracy normalnej (100% obc.)	>93%
5	Sprawność w trybie podwyższonej sprawności (100% obc.)	>98%
6	Współczynnik mocy	Min. 0,9
7	Czas przełączenia na baterię	0 ms
8	Liczba, typ gniazd wyjściowych	Listwa zaciskowa + dodatkowo min. 4 gniazda IEC C19 (16A) na module bypassu serwisowego.
9	Typ gniazda wejściowego	Listwa zaciskowa
10	Czas podtrzymania dla 100% obciążenia dla pf=0,9	Min. 8 min
11	Czas podtrzymania przy 50% obciążenia dla pf=0,9	Min. 21 min
12	Czas podtrzymania przy 1.5kW obciążenia dla pf=0,9	Min. 49 min
13	Dodatkowe baterie	Możliwość dodania do min. 11 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 190 minut dla 100% obciążenia przy pf=0,9
14	Wejściowe napięcie znamionowe	380/400/415 V (trójfazowe)
15	Tolerancja napięcia prostownika	305-480 V bez obniżania mocy (pomiędzy 175–480V przy obniżeniu mocy)
16	Całkowite odkształcenia napięcia THDu	<2% dla obciążenia liniowego, <5% dla obciążenia nieliniowego
17	Częstotliwość znamionowa	50/60 Hz autodetekcja
18	Tolerancja częstotliwości	40– 70 Hz
19	Kształt napięcia	Sinusoidalny
20	Napięcie znamionowe wyjściowe	200/208/220/230/240V do wyboru przez użytkownika (jednofazowe)
21	Zakres zmian napięcia	+/-1% napięcia nominalnego

22	Częstotliwość wyjściowa	50/60 Hz +/-0,5%
23	Odkształcenia prądu wejściowego przy jego wartości znamionowej THDi	<5%
24	Współczynnik szczytu	3:1
25	Dopuszczalny zakres współczynnika mocy obc. Liniowego	0,5 indukcyjny - 0,5 pojemnościowy
26	Baterie wymieniane przez użytkownika "na gorąco"	Tak
27	Ochrona przed przeładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
28	Ochrona przed głębokim rozładowaniem	Tak
29	Okresowy automatyczny test baterii	Tak
30	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni.
31	Zdolność zwarciowa	90A
32	Możliwość uruchomienia bez napięcia w sieci	Tak
33	Baterie wewnętrzne	Min. 9Ah 12V, minimum 20 szt.
34	Czas ładowania baterii do poziomu 90%	< 1,5 godz. do 90% pojemności użytkowej
35	Interfejs komunikacyjny	min. 1x USB
		min. 1x RS232 DB-9 żeński (HID)
		styki przekaźnikowe
		miniport wyłącznik ON/OFF
		min. SNMP/Ethernet
36	Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa) Dostarcza informacji o : stanie pracy urządzenia, stanie obciążenia, pomiarach i ustawieniach. Funkcje ustawień i odczytów: lokalne, wyjścia (napięcie wyjściowe, częstotliwość wyjściowa), baterii (test baterii), pomiary i dane (numer seryjny, napięcie i częstotliwość wejściowa i wyjściowa, poziom obciążenia, pozostały czas podtrzymania, wydajność, zużycie energii).
		Poziomy rząd przycisków sterowania
		Poziomy rząd wskaźników stanu: zasilanie z siec(zielony), trybu bateryjnego (żółty), usterki (czerwony)
		Sygnalizator akustyczny
37	Sygnały akustyczne min.	Awaria
		Niski stan naładowania baterii
		Przeciążenie
		Serwis
38	Przyciski sterujące i wskaźniki diodowe LED min.	Przycisk Escape (anulowanie)
		Przyciski funkcyjne (przewijanie w górę i w dół)
		Przycisk Enter (potwierdzający)

		Przycisk ON/OFF załączenia i wyłączenia
		LED trybu zasilania z siec i(kolor zielony)
		LED trybu baterii (kolor żółty)
		LED usterki (kolor czerwony)
39	Typ obudowy	Uniwersalna Tower/Rack 6U
40	Wyposażenie standardowe min.	UPS, instrukcja obsługi (CD), instrukcja bezpieczeństwa, inst. „Quick start”
		2 x kabel wyjściowy IEC
		1 x kabel szeregowy RS-232
		1 x kabel komunikacyjny USB
		1 x CD Oprogramowanie
		uchwyty kablowe
		zestaw szyn montażowych 19’
		podstawki do montażu wieżowego
		1x karta sieciowa SNMP/Ethernet
41	Dane techniczne karty SNMP min.	Network Support: Ethernet /10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/
		Tymczasowe hasła: Nadawanie użytkownikowi dostępu za pomocą konta. Konto może wygasać po odpowiedniej, wprowadzonej liczbie dni (hasło przestaje być aktywne). Blokowanie konta: Po określonej liczbie nieudanych prób wpisania hasła lub określonej liczbie dni.
		Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI
		Kamptybilność: SNMP v1/v3 i IP v4/v6
		Interfejs: HTML5
		Adresowanie IP: DHCP/BootP/Manualne
		Szyfrowanie: pakiet szyfrów TLS 1.2 z minimum SHA256
		Dostępny port USB (microUSB - port serwisowy)
42	Dołączone oprogramowanie	Tak, monitorujące i zarządzające UPS, umożliwiające automatyczne zamykanie serwerów zasilanych z systemu i pracujących pod kontrolą systemów operacyjnych: - Windows: 7 / 8 / 2008 / Vista - Linux: Debian GNU Linux: Lenny, SUSE/Novell: SLES 11, OpenSUSE 11.2, Redhat Enterprise Linux: RHEL 5.3, 5.4, 5.5, Fedora core 12 Ubuntu: 10.04 - VMWare: vCenter / ESXi 5.1 Oprogramowanie musi posiadać funkcjonalność integracji (plug-in) z platformą wirtualizacyjną Vmware: vCenter Server.
43	Zgodność ze standardem Energy Star	Tak
44	Poziom hałasu w odl. 1m	do 48 dBA dla pracy normalnej

45	Bypass elektroniczny automatyczny i bypass mechaniczny serwisowy z dwupozycyjnym przełącznikiem obrotowym (standardowo)	Tak
46	Gwarancja	min. 36 miesięcy od daty uruchomienia, obejmująca wszystkie konieczne do utrzymania gwarancji przeglądy eksploatacyjne.

b) Przełącznik ATS – 1 szt.:

- Automatyczny przełącznik źródeł zasilania umożliwi zasilanie z 2 różnych źródeł. Jeżeli jedno źródło zasilania ulegnie awarii, to źródło rezerwowe zostanie przyłączone w typowym czasie przełączenia wynoszącym max. 8ms, do podłączonego sprzętu.
- Prąd znamionowy: min. 16A
- Napięcie znamionowe / częstotliwość wejściowa: 208/220/230/240 V ; 50/60 Hz.
- Gniazda wejściowe: min. 2 IEC C20 + 2 przewody wejściowe.
- Gniazda wyjściowe: min. (8 IEC C13 + 1 IEC C19).
- Wyświetlacz LCD: Tak.
- Dodatkowe wyposażenie: Karta komunikacyjna typu SNMP umożliwiająca zdalne i lokalne monitorowanie stanu pracy oraz zarządzenie przełącznikiem zasilania.
- Gwarancja: min. 36 miesięcy od daty uruchomienia, obejmująca wszystkie konieczne do utrzymania gwarancji przeglądy eksploatacyjne.

2. Etap II: Oprogramowanie i wyposażenie serwerowni Uniwersyteckiego Centrum Informatyzacji – OPROGRAMOWANIE o minimalnych parametrach:

2.1. Oprogramowanie wirtualizacyjne o minimalnych parametrach – 1 kpl:

1) Należy dostarczyć licencje na oprogramowanie wirtualizacyjnego wraz z oprogramowaniem zarządzającym umożliwiającym zcentralizowane zarządzanie wirtualną infrastrukturą. Należy dostarczyć licencje serwerowych systemów operacyjnych do uruchomienia maszyn wirtualnych wraz z licencjami dostępowymi dla uruchomienia aplikacji (min. 2050 użytkowników). Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na uruchamianie wirtualnych środowisk serwerowego systemu operacyjnego w usłudze hostowanej platformy serwerowego systemu operacyjnego. Szczegółowe wymagania co do wymaganego systemu operacyjnego zostały podane poniżej.

2) Dostarczone licencje na oprogramowanie wirtualizacyjne wraz oprogramowaniem zarządzającym będzie zainstalowane na dostarczonej infrastrukturze serwerowej i ma swoim licencjonowaniem obejmować tę infrastrukturę. System wirtualizacji ma być kompatybilny z systemem wirtualizacji posiadanym przez Zamawiającego Vmware Vsphare tj. musi umożliwić bez zastosowania konwerterów odtwarzanie maszyn wirtualnych działających na obecnym środowisku Zamawiającego.

3) Minimalne parametry oprogramowania wirtualizacyjnego:

a) Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

b) Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

c) Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.

d) Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w min. 576 logicznych wątków oraz do min. 12 TB pamięci fizycznej RAM.

e) Oprogramowanie do wirtualizacji musi zapewnić:
   - możliwość skonfigurowania maszyn wirtualnych w zakresie 1-128 procesorów.
   - możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB,

- możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM,
- możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych,
- możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.

f) Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.

g) Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.

h) Rozwiązanie musi być kompatybilne i wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003/R2, Windows Server 2008/R2, Windows Server 2012/R2, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Oracle Enterprise Linux, Debian GNU/Linux, CentOS, FreeBSD, Asianux, NeoKylin Linux, CoreOS, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X.

i) Rozwiązanie musi umożliwiać
- przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji,
- udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.

j) Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu min. HTML5.

k) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.

l) Oprogramowanie do wirtualizacji powinno zapewnić
- możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy,
- możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

m) Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi posiadanymi przez Zamawiającego.

n) Rozwiązanie musi zapewniać:
- mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. Mechanizm ten jest elementem składowym rozwiązania i nie wymaga dodatkowej licencji na system operacyjny.
- mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.

o) Rozwiązanie musi mieć:
- możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie,
- możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie.

p) Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

q) Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym

oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.

r) System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.

s) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.

t) Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

u) Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek. Rozwiązanie musi obsługiwać mechanizmy przełączania ścieżek SAN dostarczane przez firmy trzecie.

v) Rozwiązanie musi mieć możliwość:
   - automatycznego równoważenia obciążenia serwerów fizycznych poprzez przenoszenie pracujących wirtualnych maszyn pomiędzy nimi. Mechanizm ten musi być wyposażony w możliwość definiowania reguł przenoszenia np. przeniesienie maszyny wirtualnej wymusza przeniesienie innej lub równoważenie następuje w obrębie zdefiniowanych grup wirtualnych maszyn pomiędzy wybranymi serwerami fizycznymi,
   - oszczędzania energii elektrycznej poprzez automatyczne wyłączenie wskazanych serwerów fizycznych w przypadku braku obciążenia generowanego przez wirtualne maszyny i automatycznego ich włączenia w sytuacji wzrostu obciążenia,
   - automatycznego równoważenia obciążenia fizycznych zasobów dyskowych poprzez przenoszenie zwirtualizowanych dysków pracujących maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm ten musi być wyposażony w możliwość definiowania reguł przenoszenia np. przeniesienie zwirtualizowanych dysków maszyny wirtualnej wymusza przeniesienie zwirtualizowanych dysków innej lub zwirtualizowane dyski pojedynczej maszyny wirtualnej będą znajdowały się na tym samym lub różnych fizycznych zasobach dyskowych.

w) Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym.

x) Gwarancja min. 36 miesięcy wraz z subskrypcjami.

4) Szczegółowe wymagania systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

a) Możliwość wykorzystania nielimitowanej liczby rdzeni logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.

b) Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.

c) Możliwość budowania klastrów składających się z 64 węzłów.

d) Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.

e) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości.

f) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.

g) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
- pozwalają na zmianę rozmiaru w czasie pracy systemu,
- umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- umożliwiają zdefiniowanie list kontroli dostępu (ACL).

h) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

i) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
j) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
k) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
l) Możliwość wykorzystania standardu http/2.
m) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
n) Dostępne dwa rodzaje graficznego interfejsu użytkownika:
- Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
- Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

o) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
p) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
q) Mechanizmy logowania w oparciu o:
- Login i hasło,
- Karty z certyfikatami (smartcard),
- Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).

r) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
s) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
t) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
u) Dostępność bezpłatnych narzędzi umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
v) Serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
w) Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
x) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania):
- Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
- Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
  - Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
  - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
  - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
- Zdalna dystrybucja oprogramowania na stacje robocze.
- Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
- Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  - Dystrybucję certyfikatów poprzez http,
  - Konsolidację CA dla wielu lasów domeny,
  - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
  - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
- Szyfrowanie plików i folderów.
- Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.

- Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- Serwis udostępniania stron WWW.
- Możliwość wsparcia dla protokołu IP w wersji 6 (IPv6),
- Możliwość wsparcia dla algorytmów Suite B (RFC 4869),
- Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
- Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- Mechanizmy wirtualizacji mające wsparcie dla:

– Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
– Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
– Obsługi 4-KB sektorów dysków,
– Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
– Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
– Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode),
– Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

y) Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
z) Możliwość wsparcia dla rozwiązania Kubernetes.
aa) Możliwość automatycznej aktualizacji w oparciu o publikowane poprawki. Dostępność do bezpłatnego rozwiązania umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
bb) Możliwość wsparcia dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
cc) Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
dd) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
ee) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
ff) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
gg) Mechanizm konfiguracji połączenia VPN do platformy Azure.
hh) Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
ii) Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.

2.2. Oprogramowanie do wykonywania kopii zapasowych maszyn wirtualnych i maszyn fizycznych o minimalnych parametrach – 1 kpl.:

1) Należy dostarczyć dla całego oferowanego środowiska serwerowego wraz z oferowanym systemem wirtualizacji oraz instancjami serwerów fizycznych oprogramowanie wraz z odpowiednimi licencjami do tworzenia kopii zapasowych. Dostarczone licencje należy zainstalować na istniejącym serwerze backupowym oraz zintegrować z istniejącym środowiskiem backupowym Zamawiającego. System do tworzenia kopii zapasowych ma być kompatybilny z systemem do tworzenia kopii zapasowych posiadanym przez Zamawiającego tj. musi umożliwić bez zastosowania dodatkowych narzędzi odtwarzanie backupów działających na obecnym środowisku Zamawiającego.
2) Wymagania minimalne dla oprogramowania do tworzenia kopii zapasowych (nowo dostarczane środowisko serwerowe):
a) Oprogramowanie backupowe musi:

- współpracować z dostarczonym oprogramowaniem wirtualizacyjnym. Wszystkie funkcjonalności w specyfikacji muszą być dostępne dla dostarczanej platformy wirtualizacyjnej, chyba, że wyszczególniono inaczej,
- współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami,
- współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami,
- zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V,
- być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej,
- tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków,
- mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji,
- pozwalać utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w takiej puli.

b) Oprogramowanie nie może:

- przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

c) Oprogramowanie musi zapewniać:

- backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
- mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie

d) Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.

e) Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) używanych przez Zamawiającego.

f) Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.

g) Oprogramowanie musi mieć:

- wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji,
- wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.

d) Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza.

e) Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)

f) Oprogramowanie musi:

- posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych,
- wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych,
- oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych,
- automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora,
- wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
- mieć możliwość wydzielenia osobnej roli typu tape server,

- mieć możliwość kopiowania backupów do lokalizacji zdalnej,
- mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son),
- wspierać BlockClone API w przypadku użycia posiadanych przez Zamawiającego serwerowych systemów operacyjnych Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu,
- mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji,
- umożliwiać przechowywanie punktów przywracania dla replik,
- umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding),
- posiadać takie same funkcjonalności replikacji dla Hyper-V,
- wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN),
- dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere,
- przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing),
- umożliwiać 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 niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania,
- pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami,
- umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków,
- umożliwić odtworzenie plików 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,
- mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V,
- wspierać odtwarzanie plików z następujących systemów plików:
  - min. Linux (ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs),
  - min. BSD (UFS, UFS2),
  - min. Solaris (ZFS, UFS),
  - min. Mac (HFS, HFS+),
  - min. Windows (NTFS, FAT, FAT32, ReFS)
  - min. Novell OES (NSS).
- wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces,
- umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej,
- wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
- wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat,
- wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia,
- indeksować pliki w celu szybkiego wyszukiwania plików w plikach backupowych,

- wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN,
- umożliwiać stworzenie laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

g) Oprogramowanie umożliwia 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.

h) Oprogramowanie musi:

- mieć mechanizmy dla replik w dostarczanym środowisku wirtualnym,
- umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

3) Wymagania minimalne dla oprogramowania do tworzenia kopii zapasowych (min. 7 instancji serwerów fizycznych min. opartych o środowisko Windows), Agent dla serwerów fizycznych:

a) Rozwiązanie musi:

- wykonywać kopię zapasową systemu Windows wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego,
- być kompatybilne i współpracować z dostarczonym serwerowym systemem operacyjnym,
- wspierać wykonywanie kopi zapasowych następujących systemów plików:
  - Min. NTFS,
  - Min. ReFS,
  - Min. FAT32.
- mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą),
- wspierać systemy oparte o Microsoft Failover Cluster,
- wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów,
- wspierać backup podłączonych dysków USB,

b) Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym,

c) Rozwiązanie musi:

- pozwalać na przechowywanie kopii zapasowych na co najmniej:
  - 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,
  - Zcentralizowanym repozytorium danych,
  - Bezpośrednio na zasobach Chmury,
  - Microsoft OneDrive/OneDrive for Business.
- wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone,
- wspierać kontrolę pasma sieciowego,
- wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych,
- wspierać ograniczenia wykonywania backupów dla połączeń VPN,
- wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych,
- wspierać technologię BitLocker,
- wspierać uruchamianie z nośnika odtwarzania. Nośnik odtwarzania musi być automatycznie tworzony przez Rozwiązanie,
- wspierać wgrywanie dodatkowych sterowników podczas odtwarzania z wykorzystaniem nośnika odtwarzania,

- wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych, umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.,
- wspierać szyfrowanie,
- wspierać możliwość wykonywania kopii zapasowych lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne,
- posiadać funkcjonalność indeksowania oraz przeszukiwania plików,
- posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego
- wspierać tworzenie kopii zapasowych wykorzystując konsolę tekstową lub CLI na maszynie zabezpieczanej
- wspierać tworzenie wielu zadań backupowych

d) Gwarancja min. 36 miesięcy wraz z subskrypcjami.

2.3. System zarządzania infrastrukturą sieciową – 1 kpl:

System zarządzania środowiskiem Datacenter o minimalnych parametrach :

1) Dostarczony System zarządzania środowiskiem datacenter musi mieć możliwość zarządzania:
- minimum 7 serwerami fizycznymi,
- minimum 1 serwerem dyskowym,
- minimum 4 przełącznikami LAN i FC,
- minimum 1 instancją zarządzającą (która stanowi maszynę wirtualną lub fizyczną)

2) System musi być skalowalny minimum 10 krotnie co do ilości urządzeń zarządzanych względem wymagań minimalnych poprzez rozbudowę licencyjną.

3) Konsola KVM każdego serwera jest wyposażona w pełen zestaw funkcji i licencji oraz udostępniać dla każdego serwera co najmniej następujące funkcjonalności:
- autoryzację dostępu do konsoli (oddzielna od systemu zarządzania oraz SSO („Single Sign On” – jednokrotnego logowania do systemu zarządzania) zintegrowane z systemem zarządzania),
- zdalne montowanie min.:
  - CD ROM/DVD ROM i obrazy ISO ww nośników,
  - Karta pamięci,
  - Fizyczny dysk twardy,
  - Obraz ISO dysku HDD.
- zdalne włączanie, wyłączanie, restart serwera,
- przeglądanie logów serwera,
- weryfikacja sekwencji startu (bootowania).

4) System zarządzania:
- musi być w pełni kompatybilny i współpracować z oferowanymi serwerami,
- opiera się o dedykowaną platformę sprzętową lub musi być maszyną wirtualną (tzw. Virtual Appliance) kompatybilną z platformą wirtualną VMware vSphere, Microsoft Hyper-V, KVM,
- posiada jeden spójny interfejs typu GUI HTML do zarządzania całym oferowanym środowiskiem sprzętowym,
- umożliwia aktualizację oprogramowanie systemowego (firmware) na serwerach w zakresie wszystkich istotnych elementów sprzętowych min: BIOS, kontrolery RAID, kontrolery KVM, karty sieciowe,
- umożliwia aktualizację oprogramowania serwerów bez przerw w dostępności systemu zarządzania,
- umożliwia definicję serwera przy pomocy logicznego profilu obejmującego konfigurację serwera w zakresie co najmniej: sieci LAN i SAN, adres MAC, adres WWNN/WWPN, sekwencja startu systemu, ustawienia BIOS, wersja BIOS/Firmware, lista sieci VLAN,
- posiada funkcje centralnego zarządzania adresami co najmniej MAC oraz adresami WWN serwerów,
- umożliwia przeniesienie logicznego profilu serwera co najmniej między dowolną parą serwerów manualnie z GUI lub automatycznie przez interfejs REST API,

- umożliwia przeniesienie logicznego co najmniej profilu z uszkodzonego serwera na inny serwer manualnie z GUI lub automatycznie przez interfejs REST API,
- posiada wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI,
- udostępnia dostęp zdalny do konsoli KVM każdego z serwerów w procesie SSO („Single Sign On” – jednokrotnego logowania do systemu zarządzania),
- musi mieć możliwość automatycznego wykrywania w sieci lokalnej serwerów przez interfejs karty zarządzającej serwera,
- musi posiadać interfejs np. typu REST API,
- udostępnia poprzez graficzny (GUI HTML), a także terminalowy (CLI/SSH) interfejs użytkownika i następujące funkcjonalności min.:

– lista komponentów serwera (inwentarz);
– wyświetlanie informacji o awariach i zdarzeniach;
– automatyczne powiadamianie o awarii poprzez email;
– archiwizacja i odtworzenie konfiguracji;
– zarządzanie z uwzględnieniem podziału grup ról użytkowników Systemu zarządzania (minimum 3 poziomy uprawnień – Administrator, Operator Systemu i Monitoring);
– integracja ze środowiskiem wirtualizacji (VMware oraz Hyper-V);
– zarządzanie mocą elektryczną całego środowiska poprzez podgląd maksymalnej i średniej wykorzystanej przez komponenty mocy energii elektrycznej;
– zarządzanie chłodzeniem całego środowiska poprzez monitorowanie temperatur na wybranych węzłach środowiska;
– obsługa szablonów definiujących logiczne profile serwerowe w tym zapisanie wzorcowej konfiguracji logicznego profilu serwerowego, a następnie tworzenie nowych profili z pierwotnie przygotowanego szablonu;
– konfigurowanie środowiska na podstawie puli wcześniej zdefiniowanych, dzielonych grup adresów LAN i SAN oraz za pomocą szablonów konfiguracyjnych interfejsów LAN i SAN;
– możliwość selektywnego oraz grupowego zdefiniowania ograniczenia poboru mocy elektrycznej wybranych zarządzanych węzłów;
– aktualizacja oprogramowania systemowego.

5) System zarządzania musi:
- mieć możliwość wyeksportowania inwentarza środowiska co najmniej w postaci pliku CSV,
- mieć możliwość monitorowanie oraz zarządzanie także macierzami oraz przełącznikami LAN,
- umożliwiać zarządzanie dostarczonymi serwerami.

6) System w ramach konfiguracji profilu dla serwera powinien umożliwiać skonfigurowanie następujących parametrów w oddzielnych politykach lub w postaci detali w sekcjach min.:
- BIOS,
- Sprzętowa karta zdalnego zarządzania (KVM),
- Wirtualizacji kart dostępu (Virtual I/O),
- Instalowany system operacyjny.

7) System powinien umożliwiać uruchomienie skryptów na zdalnych serwerach.

8) System zarządzania umożliwia:
- zdefiniowanie fizycznych lokalizacji zainstalowanego sprzętu (Data Center, piętro, szafa stelażowa),
- importowanie obrazów instalacyjnych systemów operacyjnych oraz późniejsze wykorzystanie tych obrazów do automatycznej instalacji.

9) System zarządzania musi posiadać pakiety integracyjne z następującymi systemami zewnętrznymi min.:
- Microsoft System Center Operations Manager,
- Microsoft System Center Virtual Machine Manager,
- VMware vCenter Server (Windows),
- VMware vCenter Server Appliance,
- VMware vRealize Operations

10) System zarządzania musi:

- mieć możliwość wykorzystania zdalnych repozytoriów w dostępnych w sieci lokalnej w postaci zasobów SMB/CIFS i NFS. Zasoby te powinny być podłączane do systemu zarządzania bezpośrednio z jego panelu kontrolnego,
- umożliwiać wyświetlanie alarmów i statusu z innych instancji tego samego systemu zarządzania (możliwość federacji instancji np. głównej i osobnych odpowiadających za datacenter/lokalizacje zapasowe itp.),
- umożliwiać wyświetlanie powiadomień z co najmniej jednego zewnętrznego systemu antywirusowego,
- mieć funkcjonalność opcjonalnego świadczenia usługi DHCP na potrzeby instalacji systemów operacyjnych z poziomu Systemu zarządzania,
- mieć możliwość konfiguracji własnego serwera DHCP na potrzeby obsługi procesu uruchamiania serwerów za pomocą protokołu PXE. Dalsza instalacja systemów operacyjnych w powinna odbywać się przez sieć LAN przy wykorzystaniu obrazów instalacyjnych systemów operacyjnych obsługiwanych przez System zarządzania.

11) Wbudowany serwer DHCP musie mieć możliwość konfigurowania parametrów min.:

- Podsieć,
- maska sieciowa,
- początek i koniec zakresu przydzielanych adresów IP,
- zakres rozgłoszeniowy,
- adresy serwerów DNS,
- adres bramy domyślnej

12) System zarządzania musi:

- umożliwiać wprowadzenie zarządzanych węzłów w tryb serwisowy (tzw. maintenance mode) w celu przeprowadzenie niezbędnych prac serwisowych,
- umieć wykorzystać protokół LLDP (Link Layer Discovery Protocol) do utworzenia mapy sieci LAN jeśli w kompatybilnych zarządzanych węzłach protokół LLDP jest wspierany,
- umożliwiać analizę przesyłanych pakietów sieci LAN na poziomie wirtualnych maszyn dla systemu wirtualizacji VMware oraz KVM,
- posiadać możliwość monitorowania oraz wyświetlać informację o dostępnej i zajętej przestrzeni, dla co najmniej technologii Microsoft Storage Spaces Direct oraz VMware vSAN,
- wspierać instalację za pomocą konfigurowanych profili co najmniej następujących systemów operacyjnych na wspieranych serwerach min.:

– VMware ESXi 6.0- 6.7,
– Windows Server 2008 R2,
– Windows Server 2012 / 2012 R2,
– Windows Server 2016,
– Windows Server 2019 ,
– Red Hat Enterprise Linux 6.x,
– Red Hat Enterprise Linux 7.x,
– SUSE Linux Enterprise Server 11 SP3 / SP4,
– SUSE Linux Enterprise Server 12 SP4,
– SUSE Linux Enterprise Server 15.

System zarządzania środowiskiem sieciowym o minimalnych parametrach :

1) W przypadku aktualizacji licencji Zamawiający wymaga, aby wykonawca przeprowadził migrację do najnowszej dostępnej wersji posiadanego przez Zamawiającego Systemu zarządzania środowiskiem sieciowym oraz rozbudował o moduł zarządzania dodatkowymi 100 urządzeniami sieciowymi (łącznie 300 urządzeń). Migracja i rozbudowa do najnowszej dostępnej wersji oraz zapewnienie min. 3 letniego wsparcia technicznego posiadanego przez Zamawiającego oprogramowania HPE IMC. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 24x7 oraz dostęp do poprawek i aktualizacji. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego. Wymagane jest aby wszystkie dostarczone i posiadane przez Zamawiającego przełączniki były obsługiwane w zakresie monitoringu i zarządzania przez to oprogramowanie. W szczególności wymagane jest wsparcie w zakresie: wykrywania urządzeń i prezentacji

ich topologii, alarmów, serwera syslog, archiwizacji, przywracania i porównywania konfiguracji, aktualizacji oprogramowania, konfiguracji VLAN, konfiguracji ACL.

2) W przypadku dostawy nowego systemu Zamawiający wymaga aby zaoferowane rozwiązanie posiadało następujące parametry minimalne:

a) System (platforma) do zarządzania siecią przewodową obejmująca pełne zarządzanie w/w przełącznikami, a także dotychczasową infrastrukturą zamawiającego w skład której wchodzą serie urządzeń HPE/Aruba:7500, 5120, 5400,

b) System musi:

- być zbudowany w architekturze klient – serwer,
- umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych w celu uzyskania redundancji i wysokiej wydajności. System dostarczony musi być systemem redundantnym instalowanym na minimum 2 maszynach fizycznych,
- umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled),
- umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników z wymuszeniem reguł złożoności haseł dla administratorów,
- pozwalać na hierarchizację zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów i zewnętrznego serwera uwierzytelniającego. Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń.

c) Licencja na system powinna umożliwiać zarządzanie minimum 300 urządzeniami sieciowymi różnych producentów z możliwością rozbudowy do przynajmniej 5000 urządzeń sieciowych,

d) System musi minimalnie wspierać instalację części serwerowej na platformach Windows Server 2008 SP2, Windows Server 2012 R2 oraz Red Hat Enterprise Linux 5.x/6.x.

e) System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność.

f) System zarządzania musi spełniać podstawowe funkcje min.:

- automatyczną identyfikację i wyszukiwanie urządzeń instalowanych w sieci. Możliwość ręcznego i automatycznego dodawania urządzeń,
- automatyczne wykrywanie topologii sieci z użyciem minimum protokołów SNMP, Telnet,
- monitorowanie stanu urządzeń,
- konfigurację urządzeń,
- konfigurację list dostępu (ACL) na zarządzanych urządzeniach,
- konfigurację VLANów na zarządzanych urządzeniach,
- zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania,
- funkcje przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń,
- narzędzie do zarządzania obrazami oprogramowania urządzeń,
- zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń,
- możliwość wysyłania alarmów np. mailem lub SMS’em,
- generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
- prezentację urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu każdego urządzenia,
- obrazowanie sieci w postaci hierarchicznych map (urządzania wraz z połączeniami fizycznymi i logicznymi) wraz z wizualizacją alarmów oraz wizualizacją poszczególnych szaf telekomunikacyjnych,
- podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy,
- wbudowane narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych,
- lokalizowanie użytkowników po adresie IP i MAC,
- definiowanie polityki zmieniającej ustawienia sieci w przypadku wykrycia ataku sieciowego,
- tworzenie mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym,

- tworzenie wzorców i szablonów konfiguracji na urządzenia,
- funkcję Telnet / SSH proxy umożliwiającą zarządzanie CLI przez przeglądarkę Internetową,
- funkcję zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android,
- dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową,
- niezbędne jest aby system zarządzania był w stanie podłączyć się i importować dane z LDAP / Active Directory,
- zbieranie informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, Email,
- zarządzanie siecią wirtualną poprzez integracje SOAP z VMWare VirtualCenter Server oraz Microsoft Hyper-V vManager,
- zarządzanie siecią wirtualną dla serwerów Microsoft Hyper-V poprzez profil Power shell oraz WMI,
- automatyczną aktualizację przez Internet,
- kontekstową funkcje pomocy zmieniającą zawartość w zależności od wyświetlanego kontekstu.

g) Muszą być dostępne moduły umożliwiające rozbudowę i integrację systemu o następujące funkcjonalności min.:

- Moduł pozwalający na zarządzenie infrastrukturą Wi-Fi,
- Moduł umożliwiający obsługę informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników,
- Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA,
- Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetSream v5 oraz analizy zawartości pakietów SMTP, FTP, http,
- Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS ,
- Zarządzanie dostępem zdalnym Ipsec/VPN,
- Zarządzanie Firewallami,
- Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x i serwer RADIUS,
- Zarządzanie klientami na stacjach roboczych w ramach implementacji technologii Network Access Control
- Wbudowany serwer TACACS,
- Funkcja monitorowania wydajności aplikacji,

3) Gwarancja min. 3 lata, a w jej ramach zapewnione wsparcie telefoniczne w trybie 24x7 oraz dostęp do poprawek i aktualizacji. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego.

2.4. System ochrony poczty elektronicznej o minimalnych parametrach – 1 kpl:

1) Zamawiający dopuszcza możliwość zaoferowania aktualizacji posiadanej przez Zamawiającego licencji Systemu ochrony poczty elektronicznej.

a) W ramach aktualizacji należy dostarczyć licencję systemu ochrony poczty elektronicznej o serwis EU oraz serwis IR dla posiadanego rozwiązania Barracuda Email Security Gateway 400 na okres min. 36 miesięcy od dnia 24.01.2020r.

2) W przypadku dostawy nowego systemu Zamawiający wymaga aby zaoferowane rozwiązanie posiadało następujące parametry minimalne:

a) Termin udzielenia licencji na korzystanie z zaoferowanego systemu wynosi min. 36 miesięcy od daty zainstalowania.

b) System ma posiadać minimum:

- ochronę i zabezpieczenia zarówno poczty przychodzącej jak i wychodzącej,
- zabezpieczenia przed próbom spoofingu, phisingu i spyware,
- zabezpieczenia przed atakami typu DoS (Denial of Service),
- zabezpieczenia poczty wychodzącej, w skład której wchodzi co najmniej ochrona antywirusowa oraz kontrola ilości wysłanych wiadomości przez użytkownika,
- ochronę i zabezpieczenia przed atakami typu DHA (Directory Harvest Attack).

c) Administrator posiada możliwość zainstalowania skanera antywirusowego dla minimum MS Exchange 2007/2010/2013.

d) System posiada:

- możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości przychodzących, wg której wiadomości mogą być blokowane, przesyłane do kwarantanny lub oznaczane jako spam.
- możliwość ustawiania progów na podstawie punktacji przypisanej przez algorytmy modułu antyspamowego dla wiadomości wychodzących, wg której wiadomości mogą być blokowane lub przesyłane do kwarantanny.
- możliwość analizy odcisku palca wiadomości (fingerprint).
- możliwość analizy obrazów dołączonych do wiadomości np. przy pomocy skanera OCR (Optical Character Recognition).
- weryfikację adresów URL zawartych w wiadomości z bazą danych znanych adresów URL zawierających spam. Możliwość blokowania, oznaczania, przenoszenia do kwarantanny takich wiadomości spamowych.
- możliwość korzystania z filtrów Bayesa.
- możliwość określania maksymalnej ilości połączeń z danego adresu IP, w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy zarówno poczty wychodzącej jak i przychodzącej.
- możliwość określania maksymalnej ilości wysłanych wiadomości od danego nadawcy w zdefiniowanym przez administratora przedziale czasu. Ustawienie dotyczy poczty wychodzącej.
- możliwość zdefiniowania adresów email wyłączonych ze sprawdzania maksymalnej ilości wysyłanych wiadomości w zdefiniowanym przez administratora przedziale czasu.
- możliwość ustawienia kwarantanny dla każdego użytkownika lub globalnej dla całego Systemu.
- możliwość ustawienia częstotliwości wysyłania powiadomienia do użytkownika o nowych wiadomościach przychodzących przeniesionych do kwarantanny: codziennie, raz w tygodniu lub nigdy.
- możliwość ustawienia częstotliwości wysyłania powiadomienia do użytkownika o nowych wiadomościach wychodzących od tego użytkownika przeniesionych do kwarantanny: codziennie, co tydzień, natychmiast lub nigdy.
- możliwość ustawienia ilości miejsca na dysku przeznaczonej na kwarantannę dla poczty wychodzącej.
- możliwość zdefiniowania w przypadku poczty wychodzącej jak długo wiadomości będą przechowywane w kwarantannie.
- uwierzytelnianie nadawcy wiadomości na podstawie SPF (Sender Policy Framework).
- uwierzytelnianie nadawcy wiadomości na podstawie mechanizmu DKIM (Domain Keys).
- możliwość zapobiegania niepożądanym wiadomościom bounce z wykorzystaniem metody oznaczania nagłówków wiadomości.
- możliwość korzystania z dowolnych zewnętrznych baz RBL.

e) System ma zapewniać dostęp do baz reputacyjnych , które zawierają listę znanych spamerów.

f) System posiada:

- możliwość zdefiniowania wykluczeń ze skanowania antyspamowego dla wiadomości wychodzących/przychodzących ze określonego adresu IP lub zakresu adresów IP.
- możliwość zdefiniowania akcji dla wiadomości przychodzących w przypadku gdy wiadomości zostały wysłane z określonego adresu IP lub określonej podsieci. Dostępne akcje w tym przypadku to co najmniej: blokowanie, poddanie kwarantannie lub oznaczenie wiadomości jako spam.
- możliwość zdefiniowania białej listy domen, subdomen.
- możliwość zdefiniowania czarnej listy domen, subdomen. Wiadomości przychodzące z tych domen/subdomen mogą być co najmniej blokowane, oznaczone jako spam lub przenoszone do kwarantanny.
- możliwość określenia dla jakich domen chronionych przez System poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
- możliwość określenia domen chronionych przez System , dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.
- możliwość określenia dla jakich adresów email poczta wychodząca będzie szyfrowana przy pomocy protokołu TLS.
- możliwość określenia adresów email, dla których poczta wychodząca będzie przekierowana na inny serwer pocztowy.

- możliwość blokowania wiadomości pochodzących z konkretnego kraju, do wyboru ma być minimum 9 krajów takich jak: Argentyna, Brazylia, Chile, Chiny, Kolumbia, Niemcy, Włochy, Rosja, Turcja.
- możliwość tworzenia reguł pozwalających na blokowanie, przesyłanie do kwarantanny lub oznaczenia wiadomości jako spam wiadomości pochodzących z danego hosta.

g) System powinien rozróżniać co najmniej 11 różnych zestawów znaków, różnych narodowości używanych do kodowania wiadomości mailowych. Wiadomości posiadające takie znaki mogą być blokowane, przesłane do kwarantanny lub oznaczone jako spam.

h) System ma umożliwiać bezawaryjne i bezusterkowe korzystanie użytkownikom z dodatkowego pluginu do aplikacji Microsoft Outlook.

i) System posiada:

- możliwość konfiguracji ilości miejsca na dysku przeznaczonego na kwarantannę każdego użytkownika. Niezależnie od tego ustawienia Systemu nie powinny usuwać wiadomości młodszych niż 3 dni.
- możliwość konfiguracji ilości dni przechowywania wiadomości w kwarantannie użytkownika.
- możliwość uruchomienia SMTP over TLS zarówno dla połączeń wychodzących jak i przychodzących.
- możliwość wymuszenia zgodności protokołu SMTP z RFC 821.
- możliwość blokowania wiadomości, które nie używają FQDN (fully-qualified domain name) w polu ‘From’ adresu.

j) Kontrola Treści**.** System posiada kontrolę zawartości załączników po:

- typie pliku, co najmniej następujące typy: MS Access, MS Excel, MS Word, Adobe PDF, MS PowerPoint, Windows exe, Windows Script. Skaner sprawdza również archiwa pod kątem obecności zdefiniowanych typów pliku,
- nazwie pliku lub rozszerzenia pliku, definiowane przez administratora,
- typie MIME pliku, definiowane przez administratora zgodnie ze standardem RFC.

k) Dostępne akcje w przypadku kontroli załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:

- poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
- poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.

l) Dostępne akcje w przypadku spakowanych, zabezpieczonych hasłem załączników wiadomości mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:

- poczta przychodząca: blokowanie, przeniesienie do kwarantanny,
- poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie, przekierowanie na inny serwer.

m) System posiada możliwość tworzenia reguł, przy pomocy wyrażeń regularnych filtrujących wiadomości po temacie, nagłówku i treści wiadomości. System posiada możliwość tworzenia takich reguł zarówno dla wiadomości przychodzącej jak i wychodzącej. Dostępne akcje mają być rozdzielone ze względu na pocztę przychodzącą i wychodzącą:

- poczta przychodząca: blokowanie, przeniesienie do kwarantanny, oznaczenie wiadomości, dodanie do białej listy,
- poczta wychodząca: blokowanie, przeniesienie do kwarantanny, zaszyfrowanie wiadomości, dodanie do białej listy, przekierowanie na inny serwer.

n) System posiada minimum 4 predefiniowane reguły poczty wychodzącej, filtrujące wiadomości co najmniej po temacie, nagłówku i treści wiadomości.

o) Ochrona antywirusowa. System ma zapewniać skanowanie antywirusowe poczty przychodzącej przy pomocy minimum 3 różnych silników antywirusowych działających jednocześnie.

- System posiada możliwość weryfikacji odcisku wiadomości lub wirusa z bazą danych, jeżeli informacje na temat tej wiadomości lub wirusa nie zostały odnalezione w lokalnej bazie.

p) ATP. System musi posiadać mechanizm wykrywania ataków typu phishing z wykorzystaniem bazy danych w chmurze .

- System musi posiadać mechanizm analizy adresów URL znajdujących się w treści wiadomości jak i w załącznika do niej dodanych. Mechanizm ten musi wykorzystywać bazę danych w chmurze .

- System musi posiadać mechanizm wykrywania podejrzanych adresów URL w treści wiadomości I zastępowania ich bezpiecznym adresem URL.
- System musi posiadać mechanizm wykrywania ataków typu typosquatting (modyfikacji znanych adresów URL poprzez np. zmianę kolejności liter) i zastępowania ich prawidłowymi adresami URL.
- System musi posiadać mechanizm sandboxingu w chmurze rozwiązania.

q) Administracja. System posiada możliwość przywrócenia poprzednich zainstalowanych wersji firmware: ma być możliwość przywrócenia do wcześniej zainstalowanej wersji firmware lub do wersji, która została zainstalowana fabrycznie.

- System posiada możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur wirusów.
- System posiada możliwość przywrócenia poprzednio zainstalowanej bazy sygnatur antyspamowych.
- System posiada możliwość konfigurowania za pomocą graficznego interfejsu dostępnego przez przeglądarkę internetową.
- Interfejs administratora ma być dostępny co najmniej w 16 różnych językach w tym w języku polskim.
- System posiada możliwość określenia czy administratorzy mają dostęp do interfejsu dostępnego przez przeglądarkę tylko poprzez protokół https.
- System posiada możliwość klastrowania w trybie active/active lub active/passive.
- System posiada możliwość integracji z usługami katalogowymi LDAP oraz Active Directory przynajmniej do weryfikacji docelowych odbiorców przychodzących przesyłek pocztowych.
- System posiada możliwość uruchomienia dla użytkowników mechanizmu SSO (Single Sign On).
- System posiada możliwość przeprowadzenia diagnostyki poprzez interfejs graficzny przy użyciu narzędzi takich jak np: ping, telnet, dig, tcpdump, traceroute.
- System posiada możliwość uruchomienia bezpiecznego, szyfrowanego połączenia z działem wsparcia technicznego na życzenie administratora.
- System posiada możliwość tworzenia kopii zapasowej konfiguracji Systemu, ustawień wszystkich lub wybranych użytkowników.
- Kopie zapasowe mają być tworzone na żądanie lub eksportowane zgodnie z harmonogramem na zdefiniowany serwer ftp i smb.
- System posiada możliwość określenia maksymalnej liczby plików kopii zapasowej przechowywanej na serwerze ftp i smb.
- System posiada możliwość tworzenia kopii zapasowej baz danych filtrów Bayesa, dla całego systemu lub dla poszczególnych użytkowników.
- System posiada możliwość skonfigurowania adresu email, na który będą przesyłane kopie każdej wiadomości przychodzącej lub wychodzącej z Systemu.
- System posiada możliwość eksportowania logów na zewnętrzny serwer (syslog).
- System posiada możliwość zapewnienia wsparcia dla SNMP.

3) Serwis.

a) Oferowane rozwiązanie Systemu musi posiadać minimum trzyletnią licencję obejmującą aktualizacje mechanizmów bezpieczeństwa co najmniej w zakresie:

- Sygnatur antyspamu,
- Sygnatur wirusów,
- Bazy danych reputacji,
- Analizy fingerprint,
- Analizy intencji,
- Reguł spamu obrazkowego,
- Reguł spamu tradycyjnego.

b) W czasie obowiązywania licencji na oferowany system Zamawiający ma prawo do wykonywania nielimitowanej liczby aktualizacji (ang. *firmware upgrade*).

c) Zamawiający może zgłaszać sprawy z zakresu pomocy technicznej kontaktując się poprzez dedykowany adres email lub dedykowany numer infolinii.

d) Jeżeli oferowany System ochrony poczty przed spamem wymaga dostarczenia odpowiedniego urządzenia do zainstalowania i obsługi systemu to Wykonawca jest zobowiązany dostarczyć niniejsze urządzenie, ponieważ Zamawiający nie dysponuje takim urządzeniem. Na dostarczone urządzenie Wykonawca jest zobowiązany udzielić min. 36 miesięcy gwarancji liczonej, od dnia podpisania przez obie strony protokołu odbioru (bez zastrzeżeń) przedmiotu zamówienia.
e) Zamawiający wymaga, aby dostarczony sprzęt posiadał następujące parametry minimalne:
- Obudowa rack
- Minimalna liczba interfejsów sieciowych Systemu to co najmniej 1 interfejs 1 Gigabit.
- Urządzenie wyposażone w redundantną macierz dysków typu RAID.
- System i urządzenie zapewnia obsługę nieograniczonej ilości użytkowników.
- Urządzenia posiada minimum 60GB ilość przestrzeni dyskowej przeznaczonej na kwarantannę
- Urządzenia posiada minimalna wielkość cache dla logów to 24 GB.
- Urządzenia posiada Deklarację zgodności CE.

f) Gwarancja powinna być świadczona przez autoryzowany serwis lub osoby na koszt Wykonawcy w siedzibie Zamawiającego, a jeżeli jest to technicznie niemożliwe to wszelkie działania organizacyjne i koszty z tym związane ponosi Wykonawca.
g) Odpowiedzialność z tytułu gwarancji jakości obejmuje zarówno wady powstałe z przyczyn tkwiących w przedmiocie zamówienia w chwili dokonania odbioru przez Zamawiającego jak i wszelkie inne wady fizyczne, powstałe z przyczyn, za które Wykonawca ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
h) W czasie obowiązywania licencji Zamawiający ma dostęp do wsparcia technicznego świadczonego w systemie 24 godziny/dobę przez 7 dni w tygodniu.
i) W razie wystąpienia wady urządzenia, wykonawca w ramach ważnej licencji przeprowadzi jego wymianę na nowy model. Wykonawca dostarcza nowe urządzenie w następnym dniu roboczym po potwierdzeniu wady.
j) Wykonawca jest zobowiązany do uznania reklamacji wad ukrytych i naprawy przedmiotu umowy lub jego wymiany na wolny od wad na warunkach określonych wyżej.

2.5. System monitorowania serwerowni o minimalnych parametrach – 1 kpl:

1) Na potrzeby zdalnego monitoringu parametrów środowiskowych w pomieszczeniu serwerowni oraz powiadamiania o przekroczeniu zdefiniowanych progów alarmowych krytycznych dla działania serwerowni parametrów należy dostarczyć, skonfigurować i uruchomić system monitoringu środowiskowego realizujący poniższe funkcje:
2) Po uruchomieniu system musi co najmniej:
a) wykonywać pomiar temperatury i wilgotności, w co najmniej 3 miejscach serwerowni (w co najmniej trzech szafach IT),
b) sygnalizować obecność dymu,
c) sygnalizować detekcję ruchu,
d) sygnalizować otwarcie drzwi,
e) przekazywać informację o alarmie z UPS (dwóch zasilaczy),
f) sygnalizować obecność wody na posadzce pod szafami,
g) umożliwiać powiadomienia, co najmniej SMS, email, SNMP,
h) umożliwiać zarządzanie za pomocą WEB, TELNET/SSH, USB, SERIAL PORT,
i) kontroler musi posiadać, co najmniej 5 konfigurowalnych wejść cyfrowych i co najmniej 2 wyjścia,
j) mieć możliwość rozbudowy w przyszłości o dodatkowe porty I/O cyfrowe oraz czujniki środowiskowe;
k) mieć dwa niezależne zasilania,
l) umożliwiać instalację w szafie 19”, i zajmować wysokość max. 1U.
3) Minimalne wymagania dotyczące systemu:
a) System do kontroli krytycznych parametrów środowiskowych takich jak wilgotność, temperatura, zasilanie, wycieki wody, włamanie i dym. System informuje o przekroczeniu ustalonego zakresu wartości ostrzegawczej bądź alarmowej.
b) Wymagania minimalne dla sytemu kontroli:
- Umożliwia monitorowanie warunków środowiska i bezpieczeństwa serwerowni poprzez sieć IP.

- Obsługiwane sensory:
- Min. 5 portów do dołączenia sensorów dobieranych do indywidualnych potrzeb.
- Min. 5 portów do dołączenia sensorów z wyjściem dwustanowym (zero-jedynkowym).
- Min. 8 czujników temperatury / wilgotności wyniesionych siecią IP (sensors over IP)
- Min. 2 wbudowane sensory - temperatury i wilgotności.
- Min. dwa porty przekaźnikowe do sterowania zewnętrznymi urządzeniami. Stan przekaźnika może zostać zmieniony automatycznie po pojawieniu się alarmu lub też manualnie przez użytkownika. Możliwość sterowania zewnętrznymi urządzeniami poprzez komendy protokołu SNMP.
- Bieżąca obsługa sieciowych video kamer IP zlokalizowanych w różnych placówkach.
- Podgląd na żywo monitorowanego obiektu z dowolnego miejsca w dowolnym czasie wraz z wyświetleniem parametrów środowiskowych. Rejestracja wideo może zostać wywołana przez definiowalne w systemie wydarzenia alarmowe
- Funkcja monitorowania do 64 urządzeń sieciowych IP za pomocą komendy "ping".
- Alarm wysyłany jest gdy urządzenie nie dopowiada na komendę.
- Tworzenie wielorakich alarmów indywidualnie dla każdego zainstalowanego czujnika.
- Alarm wyzwalany jest przez przekroczenie założonych parametrów pojedynczego czujnika lub też kombinację kilku warunków połączonych ze sobą a składających się na tzw. alarm inteligentny.
- Alarmy umieszczane są w systemowym dzienniku zdarzeń, dostępnym poprzez interfejs użytkownika.
- Automatyczna konfiguracja sieci z protokołem DHCP (ustawienie statycznego adresu IP w przypadku braku serwera DHCP)
- Min. 1x port USB do podłączenia modemu USB lub do zapisywania dziennika zdarzeń w pamięci typu flash.
- Opcjonalnie moduł z wbudowaną bateria podtrzymującą zasilanie (Zanik zasilania i ponowne jego pojawienie się sygnalizowane jest odpowiednim alarmem)
- Zdublowane wejście zasilające w celu dołączenia dwóch niezależnych źródeł zasilania (Drugi zasilacz dostarczany wraz z urządzeniem).
- W celu zwiększenia ilości dołączonych sensorów istnieje możliwość kaskadowego łączenia do pięciu modułów monitoringu przy użyciu sieci Ethernet
- W połączeniu kaskadowym używa się pojedynczego interfejsu web-owego dla wszystkich modułów i sensorów.
- Konfiguracja i nadzór poprzez zintegrowany serwer web HTTP/HTTPS, Telnet, SSH lub interfejs szeregowy USB/RJ45
- Protokoły bezpieczeństwa min.: HTTPS, SSHv2, SSLv3, filtrowanie adresów IP, LDAPv3, szyfrowanie AES 256-bitowe, autoryzacja 16-znakowym loginem i hasłem, definiowalne ograniczenie praw dostępu poszczególnych użytkowników.

4) Zarządzanie:

a) system w pełni konfigurowalny przez przeglądarkę internetową,
b) konfiguracja progowych wartości zadziałania czujnika, czasu działania, sposobu wysyłania alarmu, formatu alarmu i zapisywania alarmu w systemowym dzienniku zdarzeń,
c) podgląd i edycja aktualnych wartości pomiarowych czujników i stanów alarmowych.
d) podgląd i edycja wpisów przechowywanych w systemowym rejestrze zdarzeń.
e) Systemowy rejestr zdarzeń przechowuje min. takie zdarzenia jak: alarmy, logowania i wylogowania użytkowników, informacje o wysyłanych mailach alarmowych
f) Przechowywanie do 1000 wpisów typu zdarzenie alarmowe lub logowanie i wylogowanie użytkowników.
g) Możliwość pobrania rejestru zdarzeń jako zwykłego pliku tekstowego.
h) Konfiguracja ustawień sieci IP (adres, maska podsieci, brama domyślna, DNS, itp.), uprawnień administracyjnych użytkowników i ustawień zapisywanych w rejestrze zdarzeń.
i) Min. 16 użytkowników może mieć dostęp do interfejsu sieciowego web jednocześnie. Uprawnienia do ustawiania progów alarmowych, reguł i metod wysyłania alarmów definiowane są indywidualnie dla każdego z użytkowników.
j) Czujniki zewnętrzne:

- Min. czujnik "kombi" do pomiaru temperatury i wilgotności jednocześnie – 3 szt.
- Stosowany do pomiary temperatury w zakresie od -20°C do +60°C.

- Stosowany do pomiary wilgotności w zakresie od 0 do 90% r.H. (wilgotności względnej).
- Dokładność pomiaru temperatury:
  - ± 0,5°C w zakresie od -20 do -10°C,
  - ± 0,4°C w zakresie od -10 do 60°C.
- Dokładność pomiaru wilgotności:
  - ± 3% w zakresie od 0 do 80% r.H,
  - ± 4% w zakresie od 80% do 90%.
- Pomiar temperatury punktu rosy.
- Długość przewodu przyłączeniowego: min. 2m.
- Czujnik przeznaczony do detekcji przewodzących wycieków płynnych.
- Czujnik wodoodporny.
- Długość przewodu czujnikowego min. 3m, max. 5m.
- Detekcja wycieków o minimalnej średnicy 1,5mm.
- Przewód czujkowy wykonany z PVC z elementami stali nierdzewnej.
- Czujnik dymu:
  - Czułość na dym: 0,5 dB/m ±0,1 dB/m.
- Czujnik stosowany w zakresie temperatur od -10°C do +50°C.
- Funkcja auto-reset po ustaniu przekroczenia wartości alarmowej.
- Czujnik dostarczony wraz z zestawem montażowym.
- Czujka ruchu.
- Wyposażona w podwójny mechanizm wykrywania: czujnik podczerwieni - PIR z podwójnym pyroelementem oraz czujnik mikrofalowy.
- Niezależna, płynna regulacja obu czujników.
- Funkcja antymaskingu realizowana przez tor mikrofalowy.
- Kontaktron magnetyczny.
- Montaż powierzchniowy.
- Klasa ochrony obudowy min. IP 43.
- Sygnalizacja zdjęcia pokrywy.
- Temperatura pracy w min. zakresie -40°C – +70°C
- Modem GSM:
  - Umożliwiający wysłanie wiadomości tekstowej typu SMS w przypadku przekroczenia wartości alarmowej przez system monitoringu.
  - Kartę SIM do modemu obsługującą wiadomości SMS (dostarczy Zamawiający).
  - Modem z interfejsem min. USB 2.0 typ A, wtyk "męski"
  - Zakres pasma sieci co najmniej 3G: HSPA+/HSUPA/HSDPA/HSPA/UMTS(WCDMA)-2100 MHz.
  - Zakres pasma sieci co najmniej 2G: GSM/GPRS/EDGE-850/900/1800/1900 MHz.

5) W cenie oferty należy uwzględnić niezbędne elementy do uruchomienia systemu monitoringu środowiskowego w szczególności okablowanie, elementy montażowe.

6) Gwarancja min. 36 miesięcy.

2.6. Instalacja i konfiguracja

1) Powyższe oprogramowanie należy zainstalować, skonfigurować na dostarczonym środowisku opisanym w pozycji „Oprogramowanie i wyposażenie serwerowni Uniwersyteckiego Centrum Informatyzacji – sprzęt” oraz przeszkolić administratorów z obsługi danego systemu.

2) W ramach przedmiotu zamówienia należy zapewnić usługi instalacji i konfiguracji towarzyszące dostawie oraz instruktaże stanowiskowe, zgodnie z poniższymi wymaganiami minimalnymi:

a) Usługa instalacji, konfiguracji i uruchomienia oprogramowania będącego przedmiotem dostawy:

- Przed przystąpieniem do prac należy przygotować do akceptacji Zamawiającego koncepcję techniczną instalacji i harmonogram prac w zakresie oprogramowania.
- Opracowanie dokumentacji powykonawczej i zaleceń powdrożeniowych obejmujące min.:
  - Szczegółowy opis konfiguracji oprogramowania.

- Szczegółowy schemat połączeń pomiędzy systemami (w formie graficznej i opisowej).
- Procedury operacyjne dla administratorów.
- Procedury awaryjnego odtwarzania danych i konfiguracji systemu po awarii.

3) Dostarczane w ramach realizacji dokumenty, opracowania i inne materiały muszą zawierać co najmniej:

a) Koncepcję techniczną zawierającą:
- Min. zestawienie dostarczonych systemów wraz z ich wersjami,
- Min. rysunki logiczne rozwiązania,
- Min. oznaczenia połączeń logicznych,
- Min. zestawienie wymaganych wersji oprogramowania podstawowego i rozszerzeń (o ile ma to zastosowanie),
- Min. zestawienie wymaganych łat systemu operacyjnego (ang. Patch Management),

b) Opis testów zawierający minimalnie:
- Zestawienie stosowanej nomenklatury,
- Weryfikację zgodności konfiguracji poszczególnych elementów z koncepcją techniczną,
- Weryfikację zgodności konfiguracji pakietów i rozszerzeń z koncepcją techniczną (o ile ma to zastosowanie),
- Weryfikację zgodności przyjętych oznaczeń połączeń logicznych z koncepcją techniczną,

c) Dokumentacja powykonawcza i zalecenia powdrożeniowe zawierający minimalnie:
- Zestawienie stosowanej nomenklatury,
- Rysunki logiczne rozwiązania,
- Zestawienie nazewnictwa poszczególnych elementów systemu,
- Rysunki połączeń logicznych,
- Zestawienie oznaczeń połączeń logicznych,
- Zestawienie zainstalowanych wersji oprogramowania podstawowego i rozszerzeń (o ile ma to zastosowanie).

4) Instruktaż. Wykonawca jest zobowiązany do przeprowadzenia instruktażów dla 5 pracowników Zamawiającego:

a) Instruktaż z instalacji, konfiguracji i zarządzania środowiskiem oferowanego systemu wirtualizacji.
- Szkolenie powinno obejmować co najmniej następujące tematy:
- Tworzenie maszyn wirtualnych,
- Instalacja i konfiguracja zcentralizowanego zarządzania środowiskiem wirtualnym,
- Konfiguracja i zarządzanie wirtualnymi mechanizmami sieciowymi,
- Konfiguracja i zarządzanie wirtualną pamięcią masową,
- Zarządzanie maszynami wirtualnymi,
- Kontrola dostępu oraz uwierzytelniania,
- Zarządzanie i monitorowanie wykorzystania zasobów,
- Wysoka dostępność i odporność na uszkodzenia,
- Skalowalność w odniesieniu sieci, hosta, pamięci masowej,
- Zarządzanie poprawkami,
- Mechanizmy do zarządzania środowiskiem,
- Instalowanie składników systemu wirtualizacji,
- Skalowalność w odniesieniu do hostów i zarządzania nimi,
- Instruktaż musi być przeprowadzony w ośrodku uprawnionym do prowadzenia szkoleń w zakresie oferowanego systemu wirtualizacji. Uczestnik szkolenia powinien po jego zakończeniu otrzymać certyfikat ukończenia szkolenia oraz materiały szkoleniowe. Wykonawca pokrywa wszystkie koszty związane ze szkoleniem (w tym zakwaterowania, wyżywienia, dojazdu, zapewnienie infrastruktury potrzebnej do przeprowadzenia szkolenia). Warunki, miejsce i termin szkolenia muszą być ustalone z Zamawiającym.

b) Instruktaż z instalacji, konfiguracji i zarządzania środowiskiem oferowanego systemu backupu.
- Szkolenie powinno obejmować co najmniej następujące tematy:
- Wymagania i scenariusze wdrożenia systemu backupu,
- Początkowa konfiguracja,

- Tworzenie kopii zapasowych, tworzenie punktów przywracania, kopiowanie kopii zapasowych, replikacja, tworzenie zadań kopiowania maszyn wirtualnych,
- Weryfikacja backupu,
- Odtwarzanie całych maszyn wirtualnych,
- Zaawansowana ochronna danych,
- Diagnozowanie i rozwiązywanie problemów,
- Instruktaż musi być przeprowadzony w ośrodku uprawnionym do prowadzenia szkoleń w zakresie oferowanego systemu backupowego. Uczestnik szkolenia powinien po jego zakończeniu otrzymać certyfikat ukończenia szkolenia oraz materiały szkoleniowe. Wykonawca pokrywa wszystkie koszty związane ze szkoleniem (w tym zakwaterowania, wyżywienia, dojazdu, zapewnienie infrastruktury potrzebnej do przeprowadzenia szkolenia). Warunki, miejsce i termin szkolenia muszą być ustalone z Zamawiającym.

c) Instruktaż z zarządzania środowiskiem oferowanego systemu zarządzania środowiskiem sieciowym

- Szkolenie powinno obejmować co najmniej następujące tematy:
- Projektowanie topologii sieciowych,
- Zabezpieczanie dostępu do systemu zarządzania środowiskiem sieciowym,
- Konfiguracja komunikacji pomiędzy systemem zarządzania środowiskiem sieciowym a urządzeniami sieciowymi,
- Wykrywanie topologii sieciowej,
- Optymalizacja,
- Najlepsze praktyki konfiguracyjne,
- Zarządzanie wieloma konfiguracjami urządzenia, zarządzanie ACL, sieciami wirtualnymi VLAN, zasobami wirtualnymi,
- Instruktaż musi być przeprowadzony w ośrodku uprawnionym do prowadzenia szkoleń w zakresie oferowanego systemu wirtualizacji. Uczestnik szkolenia powinien po jego zakończeniu otrzymać certyfikat ukończenia szkolenia oraz materiały szkoleniowe. Wykonawca pokrywa wszystkie koszty związane ze szkoleniem (w tym zakwaterowania, wyżywienia, dojazdu, zapewnienie infrastruktury potrzebnej do przeprowadzenia szkolenia). Warunki, miejsce i termin szkolenia muszą być ustalone z Zamawiającym.

5) Szczegółowe prace instalacyjno-konfiguracyjne:

a) Na nowo instalowanych serwerach należy zainstalować system wirtualizacji tzw. hipervisor. Jako maszynę wirtualną należy zainstalować system zarządzania wirtualizacją. W środowisku wirtualizacyjnym należy skonfigurować klaster wysokiej dostępności. Połączenia do sieci LAN i SAN muszą być skonfigurowane redundantnie. W środowisku wirtualizacyjnym należy skonfigurować bezprzerwowe działanie wybranych maszyn wirtualnych. Przestrzenią dyskową dla wirtualizacji mają być dostarczane serwery dyskowy z odpowiednią ilością miejsca na dane Zamawiającego. Serwer dyskowy musi zapewniać wysoką dostępność. Podział przestrzeni dyskowej należy uzgodnić z Zamawiającym i wystawić ją według wymagań Zamawiającego.

b) Dla nowo instalowanego środowiska należy uruchomić system backupowy. System backupowy musi umożliwić uruchomienie maszyn wirtualnych z systemu backupu. Dane maszyn wirtualnych powinny byś przechowywane na jednym z uzgodnionych wolumenów serwera dyskowego nie podlegającego replikacji. Harmonogram backupów należy uzgodnić z Zamawiającym. W środowisku backupowym należy uruchomić i skonfigurować wirtualne laboratorium umożliwiające testowanie wykonywanych backupów.

c) Nowo instalowane środowisko należy zintegrować z istniejącym środowiskiem Zamawiającego w celu umożliwienia wymiany danych pomiędzy nowo instalowanymi systemami a istniejącymi. W celu integracji środowisk danych należy uwzględnić licencje na połączenie środowisk SAN i potrzebne wkładki GBIC, jeśli takie będą wymagane.

d) Szczegółowe wymagania instalacji i konfiguracja systemu backupu muszą obejmować co najmniej:

- Ustalenie maszyn wirtualnych mających podlegać systemowi backupowemu,
- Uzgodnienie polityk backupowych,
- Ustalenie miejsca przechowywania danych,
- Instalacja oprogramowania na serwerze,
- Rejestracja licencji,

- Konfiguracja powiadomień z systemu backup na uzgodnione konto pocztowe,
- Konfiguracja oprogramowania zgodnie z ustaleniami,
- Wykonanie backupów testowych,
- Weryfikacja przywracalności wybranych maszyn wirtualnych,
- Należy uruchomić skonfigurować virtualne laboratorium w celu testowania backupów i odtworzeń,
- Weryfikacja odtworzonych maszyn wirtualnych
- Dla oprogramowania do wirtualizacji Zamawiający wymaga :

– Odwzorowania obecnej struktury maszyn wirtualnych wykorzystywanych przez System ERP
– Odwzorowanie obecnej struktury maszyn wirtualnych wykorzystywanych przez kontroler domeny i powiązane systemy

e) Dla posiadanej i użytkowanej przez Zamawiającego usługi katalogowej Active Directory (AD) Zamawiający wymaga :

- aktualizacji do najnowszej wersji oprogramowania z zachowaniem dotychczasowych danych i powiązań z systemami,
- przeprowadzenie testów autoryzacji użytkowników dla systemów wykorzystujących usługę AD do autoryzacji użytkowników,
- przeprowadzenie testów integracji zgodnie z dotychczasowymi rozwiązaniami (m. in. zakładanie kont AD za pośrednictwem systemu personalizacji),
- zapewnienia działania dla wydanych aktywnych certyfikatów

6) W ramach realizacji przedmiotu zamówienia należy dokonać rekonfiguracji istniejącego firewall-a (klaster) jako rozszerzenie spójnej ochrony sieci UR. Rekonfiguracja w szczególności będzie dotyczyć min.:

a) Stworzenia dodatkowych wirtualnych interfejsów dla odpowiednich vlan-ów.
b) Konfiguracji reguł dostępowych dla każdej z nowo powstałych sieci LAN, ograniczając ruch do niezbędnego (reguły musza być analogiczne jak dla innych sieci aby tworzyły wspólny system zabezpieczeń dla całego UR)
c) Uruchomienie wszystkich wymaganych w opisie modułów do ochrony w ramach jednego kompleksowego zabezpieczenia UR.
d) Konfiguracja routingu dla nowo definiowanych sieci, które musza współpracować z posiadanymi innymi działającymi sieciami na UR i tworzyć integralna spójną sieć.
e) Wykonania analizy posiadanej infrastruktury, wynikiem której ma być dokument zawierający min.:

- Schemat logiczny infrastruktury firewall z uwzględnieniem wszystkich lokalizacji,
- Adresację urządzeń we wszystkich strefach,
- Tablicę NAT-owań wraz z tabelą wykorzystania publicznych adresów IP
- Tunele VPN zestawione między lokalizacjami (parametry)

d) Wykonanie projektu technicznego rekonfiguracji oraz dodatkowej konfiguracji obejmującego min. :

- Stworzenie dodatkowych wirtualnych interfejsów dla odpowiednich vlan-ów stworzonych w ramach realizacji przedmiotu zamówienia według wymagań Zamawiającego,
- Konfiguracji reguł dostępowych dla każdej z nowo powstałych sieci LAN, ograniczając ruch do niezbędnego,
- Uruchomienie wszystkich dostarczonych ochron oraz reguł QoS dla nowo definiowanych sieci LAN,
- Konfiguracja dostępów VPN, tak aby możliwy był dostęp do nowo dostarczonych zasobów w bezpieczny sposób z lokalizacji wyniesionych,
- Konfiguracji routingu dla nowych sieci LAN(VLAN) tak, aby spełnione były wymagania dostępowe. Opis procedur zawierający min. :

– Kolejność wykonywania instalacji,
– Wykonanie pełnych backupów istniejących konfiguracji oraz urządzeń,
– Opis zagrożeń wynikających z prac jakie mają być przeprowadzone,
– Procedurę awaryjną w razie niepowodzenia wykonania

7) Wykonanie instalacji według wykonanych przez Wykonawcę procedur musi zostać zaakceptowanych przez Zamawiającego. Szczegółowy spis urządzeń i aktualnie posiadanych wersji licencji znajduje się u Zamawiającego. Ze względów bezpieczeństwa nie będzie on podany do informacji publicznej, wgląd będzie możliwy w siedzibie Zamawiającego.

8) Rekonfiguracji sieci należy dokonać również na urządzeniach sieciowych pośredniczących (klaster IRF, urządzenia dostępowe sieci LAN).
9) Zamawiający wymaga, aby Wykonawca zapewnił wsparcie ekspertów technicznych w wymiarze 8h miesięcznie w okresie trwania gwarancji. Zamawiający zastrzega możliwość wezwania Wykonawcy do przeprowadzenia dodatkowych szkoleń, prac konfiguracyjnych w lokalizacji wskazanej przez Zamawiającego w ramach wymaganych godzin wsparcia.
10) Na wszelkie prace Zamawiający wymaga udzielenia gwarancji jakości min. 36 miesięcy.
11) Zamawiający nie dopuszcza realizacji przedmiotu zamówienia zdalnie. Wszelkie prace instalacyjno – konfiguracyjne muszą odbyć się w uzgodnionych z Zamawiającym terminach poza godzinami pracy uczelni.