Załącznik nr 6 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Informacje ogólne

1. Wykonawca zobowiązany jest do zaplanowania i skoordynowania prac w taki sposób, aby maksymalnie zminimalizować niedostępność infrastruktury teleinformatycznej dla Użytkowników.
2. Przed przystąpieniem do pracy, w terminie do 3 dni roboczych od podpisania umowy, Wykonawca przedkłada do akceptacji Zamawiającego harmonogram prac wraz z wyznaczonymi "oknami serwisowymi", w których poszczególne usługi i systemy będą niedostępne. Preferowany czas okien serwisowych to godziny i dni, w których Starostwo nie pracuje z uwzględnieniem faktu, że dostępność internetowych usług geodezyjnych powinna być całodobowa, a ich niedostępność trzeba maksymalnie minimalizować.
3. W ciągu jednego dnia roboczego Zamawiający zaakceptuje bądź odrzuci harmonogram prac wskazując zakres wymagający naniesienia poprawek. W przypadku braku akceptacji harmonogramu, Wykonawca zobowiązuje się do naniesienia poprawek w ciągu jednego dnia roboczego. Poprawiony harmonogram musi zostać przedstawiony do ponownej akceptacji przez Zamawiającego, na którą ten ma jeden dzień roboczy. Powyższy scenariusz może być powtarzany jednak nie wydłuża on czasu na realizację Zamówienia.
4. Kolejność wykonania poszczególnych zadań musi zapewniać realizację efektu zamierzonego, tj. nie można wykonać np. malowania przed montażem drzwi i pozostawić drzwi nieobrobionych.
5. Wykonawca zobowiązuje się zrealizować wszystkie prace z uwzględnieniem przepisów BHP.
6. Zamówienie będzie wykonane w następujących etapach:
   i. Modernizacja pomieszczeń serwerowni
   ii. Modernizacja systemu zasilania I klimatyzacji
   iii. Dostawa sprzętu i oprogramowania
   iv. Usługi migracji I konfiguracji
   v. Testy, dokumentacja, szkolenia
   vi. Odbiór końcowy

2. Modernizacja pomieszczenia serwerowni głównej

1. Przedmiotem zamówienia jest modernizacja pomieszczenia serwerowni przy ul. Tanowskiej 8 w Policach.
2. Parametry pomieszczenia:
    a. Poziom: –1
    b. Wielkość pomieszczenia: 4,3m x 3,45m x 2,7m (dł. x szer. x wys.)
3. W pomieszczeniu należy wykonać następujące prace:
    a. Demontaż grzejnika CO
        - Odcięcie i trwałe zaślepienie rozgałęzienia w pomieszczeniu obok
        - Demontaż grzejnika, rurek i uchwytów
        - Usunięcie i złomowanie grzejnika oraz innych pozostałości
    b. Wymiana drzwi serwerowni
        - Demontaż istniejących drzwi
        - Drzwi Lewe otwierane na zewnątrz klasy C
        - EI60 wg PN-EN-13501
        - Dymoszczelność
        - Wymiary w świetle ościeżnicy min. 1000x2000mm
        - Usunięcie i złomowanie starych drzwi oraz innych pozostałości
        - Drzwi muszą być wyposażone w zamek kluczowy
        - Kolor uzgodniony z Zamawiającym
    c. Dostawa i montaż podłogi technicznej (podniesionej) na całej powierzchni serwerowni przy ul. Tanowskiej 8.
        - Podłoga podniesiona powinna składać się z płyt o właściwościach antyelektrostatycznych. Silnie sprasowana płyta wiórowa o gęstości powyżej 700 kg/m3, spód płyty musi być pokryty blachą stalową ocynkowaną o grubości 0,5 mm, wierzch płyty aplikowany wykładziną PVC antyelektrostatyczną typu Gerflor Mipolam EL7 lub Fatra, kolory do uzgodnienia.
        - Boki płyty muszą być zabezpieczone taśmą PCV przewodzącą o grubości 0,6 mm.
        - Konstrukcja wsporcza musi być wykonana z profili C40/40 wsparta na płynnie regulowanych wspornikach stalowych ocynkowanych, klejonych do podłoża.

          Wymagane jest ponadto:
        - przystosowanie podłogi podniesionej do uziemienia,

- malowanie płynem antypyłowym,
- wykończenia listwą przyścienną z PVC,

Podłoga powinna posiadać :

- Krajowy Certyfikat Stałości Właściwości Użytkowych
- Atest Higieniczny
- Klasa obciążenia (6) 6,0 kN
- Dopuszczalne obciążenie powierzchniowe 30 kN/m^2
- Obciążenie punktowe max. 8,9 kN
- Opór elektryczny upływu podłogi Ru [Ω] $5 \cdot 10^4 \leq Ru \leq 1 \cdot 10^9$
- Klasa bezpieczeństwa 2
- Klasa reakcji na ogień B_{fl}-s1
- Klasa odporności ogniowej REI30
- Klasa ugięcia A (2,5 mm)
- Pokrycie wierzchnie wykładziną PVC antyelektrostatyczną
- Wysokość podniesienia: min 150mm
- Rampa podjazdowa od drzwi wejściowych

d. Uszczelnienie istniejących okien oraz ich trwałe szczelne zamknięcie zgodnie z normą ISO 14520 pkt 8.2.4 wraz z trwałym przysłonieniem szyb

e. Szpachlowanie nierówności ścian z wypełnieniem ubytków - w jakości równoważnej Q2

f. Malowanie pomieszczenia
   - Farba lateksowa
   - Kolor do ustalenia z Zamawiającym

2.1. Modernizacja Systemu Klimatyzacji

1. Demontaż istniejących urządzeń klimatyzacyjnych z uwzględnieniem obowiązków wynikających z Ustawy o CRO SZWO Dz. U. z 2017 poz. 1951 / Dz.U. z 2015 poz. 881 z późniejszymi zmianami oraz ustaw pochodnych wraz z (w przypadku, gdy zajdzie taka potrzeba) przygotowaniem dokumentacji do zgłoszenia wyłączenia z eksploatacji do CRO dla Zamawiającego.
2. Nowa klimatyzacja redundantna

Dla pomieszczenia serwerowni zaprojektowano układ dwóch klimatyzatorów typu split pracujące na **czynniku chłodniczym R32** o nominalnych mocach chłodniczych 20kW z jednostkami wewnętrznymi typu kanałowego pracującymi naprzemiennie, **jednostki zewnętrzne z poziomym wydmuchem powietrza**.

Dostarczony wraz system sterownik przewodowy do pracy naprzemiennej musi zapewnić następujące funkcje sytemu:

- **funkcja kaskady temperaturowej** – w przypadku wzrostu temperatury w pomieszczeniu przy pracy jednego urządzenia klimatyzacyjnego o 2,0C do 5,0C (wartość ustawiana co 1,0C) i utrzymywanie się wyższej temperatury przez czas powyżej 5 minut zostaje automatycznie włączony do pracy klimatyzator będący w stanie czuwania,
- **funkcja backup** – zabezpiecza pomieszczenie klimatyzowane przed brakiem chłodzenia w przypadku uszkodzenia klimatyzatora prowadzącego, klimatyzator czuwający załącza się w wyniku sygnału awarii z jednostki pracującej, przejmując zabezpieczenia pomieszczenia przed wzrostem temperatury zanim zadziała funkcja kaskady.

Urządzenia muszą posiadać funkcję autorestartu oraz szeroki temperaturowy zakres pracy w trybie chłodzenia w temperaturach zewnętrznych min. od -20,0C do +45,0C.

Klimatyzatory muszą posiadać klasę sezonowej efektywności energetycznej w trybie chłodzenia SEER min. 6,00. Montowany system musi posiadać certyfikat EUROVENT, który potwierdzi parametry techniczne przedstawiane w materiałach producenta. Certyfikat należy dołączyć do oferty.

Głośność - Poziom ciśnienia akustycznego każdej z jednostek zewnętrznych nie może przekraczać 57 db(A) pomiar z odległości 1,5m, dla trybu chłodzenia.

JEDNOSTKA WEWNĘTRZNA

- nominalna moc chłodnicza min. 19kW/jednostka,
- poziom ciśnienia akustycznego na najwyższym biegu wentylatora nie więcej niż49dB(A) – pomiar z odległości 1,0mb.,
- poziom ciśnienia akustycznego na najniższym biegu wentylatora nie więcej niż 36dB(A) – pomiar z odległości 1,0mb.,
- przepływ powietrza na najwyższym biegu min. 2 040,0 m3/h,
- zasilanie jednostki wewnętrznej 220V-240V – 50Hz,

Sterownik do pracy naprzemiennej musi posiadać możliwość ustawienia temperatury ze skokiem co 0,5C, pomiarem temperatury w miejscu montażu oraz programator tygodniowego czasu pracy, tryb pracy urządzenia podczas nieobecności użytkowników, sygnalizację odszraniania, sygnalizację zabrudzenia filtra, adresowanie pomieszczeń w których znajdują się jednostki.

Dodatkowo system musi być wyposażony w **złącze** umożliwiające konfigurowanie z poziomu sterownika **programowalnych wejść/wyjść**

Sygnały wejściowe - włącz / wyłącz, zezwolenie / zakaz, chłodzenia / grzanie, awaryjne zatrzymanie

Sygnały wyjściowe – chłodzenia (odszranianie), działanie wentylatora, praca wentylatora na biegu wysokim i ultra wysokim, praca wentylatora na biegu średnim i niskim, alarm przeciążeniowy jednostki wewnętrznej

3. IDU jednostek klimatyzacyjnych powinno być zainstalowane w taki sposób, aby nie znajdowało się bezpośrednio nad szafami RACK, szafami elektrycznymi, UPS'ami bądź innymi urządzeniami elektrycznymi. Szczegółowe umiejscowienie powinno być uzgodnione i przedłożone do akceptacji Zamawiającemu.
4. IDU nie mogą utrudniać poruszania się po pomieszczeniu serwerowni, otwierania szaf oraz operowania przy sprzęcie w szafach RACK.
5. ODU muszą zostać zainstalowane w taki sposób, aby były odporne na akty wandalizmu (powinny posiadać dodatkowe zabezpieczenie w postaci obudowy wykonanej z profili stalowych/krat, dodatkowo w miejscu pracy wentylatora powinna chronić go siatka stalowa z małymi oczkami bądź rozwiązania równie lub bardziej skutecznego).
6. Umiejscowienie ODU I IDU musi być przedstawione Zamawiającemu przed przystąpieniem do realizacji prac i podlega rygorowi uzgodnieniowemu, takiemu samemu jak harmonogram prac (opis w rozdziale 1 pkt. 1 SOPZ).
7. Prace, montaż, wykonanie nowej instalacji, jej napełnienie czynnikiem chłodzącym, rozruch testy i uruchomienie muszą zostać wykonane przez Autoryzowany serwis instalacyjny producenta zaoferowanych urządzeń. – do oferty należy dołączyć ważny certyfikat potwierdzający powyższy warunek.
8. Dostarczone urządzenia muszą być objęte 5 letnią gwarancją producenta lub jego autoryzowanego w Polsce przedstawiciela. Zamawiający zobowiązuje się do regularnego dokonywana przeglądów urządzeń przez cały okres użytkowania

2.2. Modernizacja Obwodów zasilania

1. Zasilanie pomieszczenia serwerowni należy wykonać przewodem 5x50mm2 bezpośrednio z głównego przyłącza elektrycznego Starostwa, znajdującego się przy wejściu B do budynku.
2. W rozdzielni głównej budynku należy przewidzieć i zabezpieczyć zdalny wyłącznik awaryjny w postaci tzw. wciskanego grzybka kompatybilnego z posiadanym UPS centralnym (EMS-1).
3. Wszystkie prace elektryczne muszą być zakończone pomiarami rezystancji izolacji i uziemienia. Odpowiednie protokoły muszą zostać niezwłocznie po zakończeniu prac przekazane Zamawiającemu.

4. Należy dokonać demontażu istniejącego UPS Eaton PowerWare 9355 30kVA z bateriami wewnętrznymi z lokalizacji przy ul. Kresowej (waga około 500kg), do serwerowni oraz wykonać podłączenie wraz z uruchomieniem ww. UPS w nowej lokalizacji wraz z zachowaniem wszelkich wymagań instalacyjnych producenta przenoszonego zasilacza UPS .
5. UPS wyposażony jest w X-slot kartę adaptera ConnectUPS-X Web/SNMP - wszystkie urządzenia serwerowe i sieciowe muszą być podłączone do skonfigurowanego oprogramowania zarządzającego UPS'a Intelligent Power Manager oraz Intelligent Power Protector pozwalającego w planowany sposób w przypadku awarii sieci elektrycznej na wyłączanie zasilanych odbiorników (piętra WGKiK w skrzydle na I piętrze budynku oraz serwerów i macierzy w serwerowni głównej)
6. UPS ponadto wyposażony jest w Detektor monitorowania środowiska EMP (Podłączany do karty SNMP/Web) oraz posiada dedykowany detektor zalania wodą (30cm) – który należy umieścić pod podłogą podniesioną tak aby maksymalnie wcześniej wykryć wszelkiego rodzaju zalania i bezpiecznie odłączyć UPS.
7. UPS dodatkowo posiada zdalny wyświetlacz LCD Eaton ViewUPS-X który należy podłączyć we wskazanym przez Zamawiającym miejscu.
8. W pomieszczeniu serwerowni należy zainstalować rozdzielnice elektryczne jak poniżej:
    a. Rozdzielnica główna
        - Złącza na podłączenie SZR-Agregat (SZR-Agregat będzie realizowany w ramach odrębnego zamówienia jednak instalowana rozdzielnica musi być gotowa na jego przyłączenie w ramach realizowanych prac);
        - Zabezpieczenia zasilania dwóch obwodów gwarantowanych;
        - Przełączniki I-O-II dla dwóch obwodów gwarantowanych;
        - Z rozdzielnicy za stykami SZR i zabezpieczeniami zasilane będą zasilacze UPS odpowiednio 1 oraz 2;
        - Z zasilaczy zasilanie ma wracać na przełączniki I-O-II (druga pozycja przełącznika ma być na stale podłączona do zasilania);
        - Z wyjść przełączników I-O-II będą zasilane dwie kolejne rozdzielnice odpowiednio Rozdz. gw . A i Rozdz. Gw. B.
    b. Rozdz. Gw. A
        - Rozdzielnica musi posiadać 5 szt. zabezpieczeń C32 dla 5 szaf rack oraz dla SZR
    c. Rozdz. Gw. B
        - Rozdzielnica musi posiadać 5 szt. zabezpieczeń C32 dla 5 szaf RACK oraz dla SZR

9. SZR
    a. Szafka SZR musi zapewnić zasilanie z dwóch obwodów naprzemiennie urządzeniom, które nie posiadają dwóch linii zasilających, tj. urządzeniom w skrzydle WGKiK PPD na parterze oraz agregatom klimatyzacyjnym;
    b. Do punktu PPD parter należy doprowadzić zasilania z ww. SZR z założeniem zasilania dwóch przełączników z zasilaczami 1600W każdy oraz dwa kable światłowodowe 12 włókien każdy: jeden z GPD drugi z PPD WGKiK odpowiedni do zastosowanych modułów optycznych stackujących switche;
    c. Na wyjściu z SZR będą znajdować się zabezpieczenia:
        - WGKiK
        - Klimatyzacja A
        - Klimatyzacja B
    d. SZR musi współpracować za pomocą MODBUS/Ethernet z zasilaczami UPS oraz klimatyzatorami tak, aby można było modyfikować scenariusze zasilania w różnych przypadkach.
10. Dostawca musi zaproponować scenariusz zasilania obejmujący priorytetyzację dostaw zasilania dla wybranych przez Zamawiającego na etapie uzgodnień przedwdrożeniowych odbiorów.
11. Należy wykonać dokumentację powykonawczą obejmującą prace elektryczne.

2.3. Instalacje Niskoprądowe

1. W serwerowni oraz w PPD w skrzydle WGKiK musi zostać zainstalowany:
    a. System kontroli dostępu
    b. System Alarmowy
    c. System Monitoringu CCTV - zastosować należy rozwiązanie umożliwiające monitoring wizyjny zarówno wejścia do serwerowni oraz punktów dystrybucyjnych, jak i ciągów komunikacyjnych. W pobliżu tych punków do rejestracji obrazu z omawianych kamer zastosowane zostanie oprogramowanie z licencjami uprawniającymi do podłączenia do 8 kamer.

2. Wymienione wyżej systemy muszą być “rozciągnięte” pomiędzy obydwie lokalizacje (GPD i PPD) oraz muszą umożliwiać rozbudowę o kolejne pomieszczenia
3. Wykonawca dostarczy licencje oprogramowania na nagrywanie do 8 kamer oraz 4 szt. kamer
4. Należy wykonać dokumentację powykonawczą obejmującą prace i instalacje niskoprądowe

3.Dostawa Sprzętu Sieciowego i Sprzętu serwerowego

3.1. Wymagania ogólne

1. Jeżeli wymagane funkcjonalności wymagają odrębnych licencji to licencje te powinny być zawarte w Ofercie.
2. Wszystkie wymagane funkcje przełączników sieciowych muszą być dostępne nie krócej niż 5 lat lub bezterminowo.
3. Wszystkie przełączniki sieciowe muszą pochodzić od jednego producenta.
4. Elementy pasywne mogą pochodzić od innych producentów niż urządzenia LAN.
5. Zamawiający wymaga, by dostarczone urządzenia były fabrycznie nowe oraz nie były używane. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
6. Zamawiający wymaga, aby całość dostarczanego sprzętu i oprogramowania pochodziła z autoryzowanego kanału sprzedaży producenta i wymaga, by przed podpisaniem umowy dołączyć certyfikat legalności produktów - oświadczenie z oficjalnego kanału dystrybucji na rynek Polski danego producenta potwierdzające, że dostawca jest autoryzowanym partnerem oraz że produkty i wsparcie oferowane klientowi pochodzą z autoryzowanego i legalnego kanału sprzedaży a także posiadają wsparcie producenta.
12. Wymagana jest minimum 5 letnia gwarancja producenta, obejmująca wszystkie elementy urządzenia, zapewniająca wysyłkę sprawnego sprzętu na podmianę nie później niż na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Przyjmowanie zgłoszeń serwisowych musi odbywać się w trybie 24godziny x7dni w tygodniu.
13. Wymagane jest zapewnienie wsparcia telefonicznego przez cały okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

3.2. Dostawa Sprzętu sieciowego

1. W ramach realizacji zamówienia Wykonawca dostarczy:
   a. Switch SAN (szt. 2)
   b. Switch LAN (szt.11)
   c. NGFW (szt. 1)

2. Zamawiający posiada NGFW FortiGate 101F. W ramach zamówienia Wykonawca dostarczy drugi identyczny firewall celem połączenia z istniejącym w klaster HA active-active wraz z niezbędnymi licencjami i subskrypcjami, nie krótszymi niż aktualnie posiadany firewall, wraz z rozszerzeniem serwisu gwarancyjnego sprzętu na czas naprawy uszkodzonego elementu w następnym dniu roboczym – urządzenie zastępcze.

3.4. Dostawa sieci WIFI wraz z konfiguracją

1. W ramach zamówienia Wykonawca uruchomi funkcjonalność sprzętowego kontrolera sieci WiFi oraz dostarczy 5szt. punktów dostępowych pracujących w standardzie minimum 802.11ac Wave 2 PoE wraz z ich instalacją na: sali sesyjnej, na korytarzu, na pierwszym piętrze, w serwerowni oraz korytarzu WGKiK zgodnie z wizją lokalną – ustalenie precyzyjnych miejsc montażu musi podlegać uzgodnieniom z Zamawiającym.

Wymagania szczegółowe dla kontrolera sieci WiFi

W ramach wdrożenia musi zostać dostarczony system pełniący funkcję kontrolera sieci bezprzewodowych, który zarządza centralnie urządzeniami typu Access Point. Kontroler musi być zrealizowany w postaci komercyjnej platformy sprzętowej lub platformy wirtualnej instalowanej na komercyjnych hypervisorach takich jak VMware, KVM. System nie powinien wymagać dodatkowych licencji na liczbę stacji klienckich.

Kontroler musi wspierać następujące funkcje:

1. Wykrywanie punktów dostępowych podpiętych do kontrolowanych segmentów sieci.
2. Pełne zarządzanie wszystkimi punktami dostępowymi z możliwością wykonania aktualizacji oprogramowania punktów dostępowych.
3. Kontroler musi podchodzić od renomowanego producenta rozwiązań bezprzewodowych ujętego w magicznym kwadracie Gartnera.
4. Kontroler musi posiadać możliwość tworzenia klastrów w celu zapewnienia redundancji.
5. Kontroler może pracować jako koncentrator VPN (IPSec, SSL) wraz z obsługą tokenów.
6. Producent kontrolera musi udostępniać klienta VPN dla urządzeń mobilnych.
7. Obsługa protokołów routingu: Statyczny, dynamiczny, policy routing, RIP, OSPF, BGP.
8. Zintegrowany serwer DHCP.
9. Konfiguracja interfejsów w trybach access i trunk
10. Mapowanie SSID do VLAN
11. Dynamiczne przypisywanie VLANów.
12. Tunelowanie ruchu do urządzeń dostępowych AP.
13. Konfiguracja sieci bezprzewodowych w trybach:
    a. Tunel (komunikacja tunelowana do kontrolera) wraz z funkcją split tunneling.

b. Local bridge (komunikacja z poszczególnych sieci radiowych mapowana lokalnie z AP do zdefiniowanych VLAN'ów).
c. Mesh.

14. Szyfrowanie komunikacji pomiędzy punktami dostępowymi AP a kontrolerem zarówno dla transmisji kontrolnej jak i ruchu klienckiego.
15. Możliwość instalacji i konfiguracji zdalnych AP, podłączonych przez łącza WAN do kontrolera z wykorzystaniem szyfrowania ruchu (minimalnie za pomocą DTLS).
16. Podtrzymanie połączeń dla SSID sieci otwartych oraz PSK na wypadek niedostępnośći kontrolera
17. Rozgłaszanie na wielu urządzeniach dostępowych AP tej samej nazwy sieci.
18. Mapowanie ruchu poszczególnych użytkowników do określonych VLAN'ów w oparciu o parametry zwracane z systemu RADIUS.
19. Natowanie ruchu poszczególnych grup użytkowników na różne adresy IP
20. Wsparcie dla Fast Roaming (protokoły 802.11k, 802.11v, 802.11r)
21. Wsparcie dla Airtime Fairness.
22. Priorytetyzację ruchu.
23. Mechanizmy przełączania stacji klienckich pomiędzy urządzeniami lub interfejsami radiowymi w celu zapewnienia jak największej efektywności sieci.
24. Monitoring stacji klienckich podłączonych do punktów dostępowych z możliwością wyświetlenia parametrów ich pracy, minimum: siła sygnału, SNR, adres IP, przepustowość, nazwa użytkownika (dla wybranych metod uwierzytelnienia).
25. Monitoring pracy punktów dostępowych z uwzględnieniem konkretnego radia oraz kanału pracy minimum: status, wykorzystanie, utylizacja.
26. Wsparcie dla protokołów: 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11n, 802.1x, 802.11ac, 802.3az, 802.3ad
27. Wsparcie dla protokołów uwierzytelniających: EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST
28. Wsparcie dla M-PSK (Multiple PSK) – obsługa wielu kluczy w obrębie jednego SSID.
29. Wsparcie dla WPA3.
30. Wewnętrzna baza, RADIUS, LDAP, TACACS+
31. Wsparcie dla zewnętrznych serwerów uwierzytelniających – Microsoft Active Directory, Microsoft IAS RADIUS server, Cisco ACS Server, Free RADIUS , Interlink RADIUS server, Steel Belted Radius
32. Wbudowany Captive Portal:
    a. Uwierzytelnienie w wewnętrznej lub zewnętrznej bazie użytkowników
    b. W pełni konfigurowalny wygląd, grafiki, język strony powitalnej
    c. Strona powitalna z akceptacją regulaminu
    d. Wiele stron powitalnych per SSID
    e. Przekierowanie do zewnętrznego captive portal'u
    f. Przekierowanie do wybranej strony po uwierzytelnieniu
    g. Kolektor adresów email
    h. Strefa dozwolona
33. Zintegrowany panel sponsora:
    a. Konfigurowalny czas wygaśnięcia kont gościnnych

b. Konfigurowalny czas rozpoczęcia działania kont gościnnych
c. Konfiguracja wielu kont na raz
d. Integracja z zewnętrznymi platformami typu self-service

34. Wbudowane mapy lokalizacji punktów dostępowych pozwalające na naniesienie punktów dostępowych na plan piętra oraz wyświetlenie parametrów ich pracy (status urządzenia, zużycie CPU oraz pamięci, stan interfejsów radiowych) - jeżeli niedostępne z poziomu kontrolera, należy zapewnić system centralnego zarządzania gwarantujący identyczną funkcjonalność.
35. Zarządzanie urządzeniem poprzez HTTPS, SSH, Telnet, konsola, SNMP (V1 & V2).

Kontroler musi wspierać posiadać wbudowane mechanizmy wykrywania i raportowania ataków na sieć bezprzewodową, takich jak:

1. Asleap Attack
2. Association Frame Flooding
3. Authentication Frame Flooding
4. Broadcasting De-authentication
5. EAPOL Packet Flooding
6. Invalid MAC OUI
7. Null SSID Probe Response
8. Spoofed De-authentication
9. Weak WEP IV Detection
10. Wireless Bridge

Dodatkowo, kontroler musi wykonywać skanowanie otoczenia w celu wykrycia obcych AP (tzw. Rouge AP) podpiętych do sieci z możliwością zakłócania ich pracy w celu eliminowania potencjalnych punktów wycieku informacji.

Skalowanie rozwiązania:

1. Maksymalna liczba zarządzanych AP – 128
2. Maksymalna liczba zarządzanych AP w trybie tunel – 64
3. Maksymalna liczba profili SSID – 128
4. Licencje – jeżeli wymaga tego model licencjonowania producenta, to konieczne jest dostarczenie wraz z urządzeniem licencji umożliwiającej obsługę maksymalnej liczby AP jaka została określona dla danego modelu urządzenia/maszyny wirtualnej.

Wymagania dotyczące Access Point – 5szt.

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -20–45°C,

   b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
   a. 2.4 GHz 802.11b/g/n,
   b. 5 GHz 802.11a/n/ac,
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Interfejs Ethernet w standardzie 10/100/1000 Base-TX,
6. Urządzenie powinno być zasilane poprzez interfejs RJ45 w standardzie 802.3af lub zewnętrzny zasilacz.
7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
   a. Tunnel,
   b. Bridge,
   c. Mesh.
8. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
   a. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
9. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
   a. MIMO – 2x2,
   b. Transmit Beam Forming (TxBF),
   c. Maksymalna przepustowość dla poszczególnych modułów radiowych:
      i. 400 Mbps;
      ii. 867 Mbps;
   d. Wymagana moc nadawania:
      i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
      ii. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
   e. Wsparcie dla 802.11n 20/40Mhz HT,
   f. Wsparcie dla kanału 80 MHz dla 802.11ac,
   g. Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
   h. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
   i. Maksymalna deklarowana liczba klientów per moduł radiowy – 512.
10. Funkcje interfejsu radiowego:
   a. Skaner częstotliwości 2.4 oraz 5 GHz,
   b. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
   c. Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,
11. Funkcje dodatkowe:
   a. Low-Density Parity Check (LDPC) Encoding,
   b. Maximum Likelihood Demodulation (MLD),
   c. Maximum Ratio Combining (MRC),
   d. A-MPDU and A-MSDU Packet Aggregation,
   e. MIMO Power Save,

f. Short Guard Interval,
g. WME Multimedia Extensions.

12. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.
13. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta

3.3. Dostawa i wdrożenie sprzętu serwerowego z oprogramowaniem

1. W ramach realizacji zamówienia należy dostarczyć następujący sprzęt:
    a. Szafa RACK z wyposażeniem – 1szt
    b. Serwery wirtualizacyjne (szt. 3)
    c. Macierz dyskowa (szt. 1)
    d. Biblioteka Taśmowa
    e. Rozbudowa istniejących serwerów NAS o moduły światłowodowe i karty 10Gb/s tak aby każdy z nich posiadał co najmniej 2 porty 10gb ethernet
    f. Rozbudowa istniejącego serwera RACK Dell PowerEdge R730 o kontroler zewnętrzny SAS
    g. Oprogramowanie
        i. Platforma Wirtualizacyjna
        ii. Oprogramowanie serwera bazodanowego wraz z licencjami dostępowymi CAL
        iii. Serwerowe systemy operacyjne wraz z licencjami dostępowymi CAL i RDS CAL
        iv. Oprogramowanie Monitoringu urządzeń sieciowych
        v. Oprogramowanie do Backupu
        vi. Oprogramowanie VMS (dołączone do kamer)

3.5. Usługi Instalacji, konfiguracji i migracji

1. W ramach realizacji przedmiotu umowy należy wykonać następujące usługi/prace:
    - Wymiana Szafy RACK TELCO oznaczona jako Szafa B wraz z patchpanelami (agregującej około 450 linii sieciowych oraz połączeń telefonicznych)
    - Demontaż istniejącej szafy RACK oznaczonej jako szafa A
    - Instalacja Nowej Szafy RACK wraz z PDU
    - Instalacja dostarczonych urządzeń sieciowych w szafie B
        - Sieć SAN musi posiadać dwa niezależne switche niepołączone ze sobą do sieci LAN

    - Sieć LAN musi posiadać 11 switchy połączonych w stos z minimalną przepustowością między członkami stosu 40gb/s
    - W serwerowni musi być zainstalowanych 6szt. switchy dla sieci LAN
    - W PPD parter musi być zainstalowany 1szt. switch sieci LAN
    - W PPD WGKiK muszą być zainstalowane 4szt. switche sieci LAN
- Instalacja dostarczonych urządzeń serwerowych w nowo instalowanej szafie A
    - Serwery muszą być podłączone do sieci LAN za pomocą redundantnych interfejsów min 10Gb/s
    - Serwery muszą być podłączone do sieci SAN za pomocą redundantnych interfejsów min. 10Gb/s
    - Serwery musza posiadać redundantne zasilanie
- Instalacja i konfiguracja dostarczonej macierzy dyskowej w nowo instalowanej szafie A
- Kontrolery macierzy muszą być podłączone wszystkimi dostępnymi portami redundantnie do przełączników SAN
- Przeniesienie serwerów RACK z lokalizacji Kresowa do lokalizacji głównej i montaż w nowej szafie A
- Instalacja serwera z demontowanej starej szafy A do Nowej szafy A
- Instalacja środowiska wirtualizacyjnego (klaster produkcyjny)
- Aktualizacja obecnych hypervizorów w serwerach przeniesionych
- Instalacja nowych kontrolerów domeny w wersji min. Windows Server 2019 na nowym środowisku serwerowym – 2szt
- Podniesienie wersji domeny do dostarczanej wersji.
- Migracja usług ze starych serwerów produkcyjnych do nowych wersji systemów operacyjnych oraz migracja na klaster produkcyjny (macierz dyskową)
- Reinstalacja systemu wirtualizacyjnego na obecnych serwerach produkcyjnych i stworzenie nowego klastra zapasowego
- Rozbudowa istniejących serwerów o odpowiednie karty HBA/NIC do podłączenia do nowo instalowanej macierzy dyskowej
- Migracja zewnętrznych krytycznych usług geodezyjnych na nowe łącza internetowe Zapewnione przez Zamawiającego
- Migracja pojedynczego urządzenia firewall do klastra produkcyjnego

- Rekonfiguracja urządzenia firewall zgodnie z najlepszymi praktykami do pracy z łączami pochodzącymi od dwóch niezależnych dostawców ISP
- Uruchomienie kontrolera sieci WiFi oraz podłączenie do niego nowo zainstalowanych AP
- Instalacja sprzętu sieciowego w szafie w PPD znajdującym się skrzydle geodezyjnym budynku
- Połączenie switchy sieci LAN zainstalowanych w serwerowni w PPD oraz w skrzydle geodezyjnym w jeden stack za pomocą portów min 40gb/s
- Migracja danych z dwóch serwerów NAS QNAP na klaster produkcyjny (zasób macierzy dyskowej)
- Instalacja urządzeń QNAP w szafie w skrzydle geodezyjnym
- Aktualizacja i w razie konieczności ponowna konfiguracja serwerów NAS QNAP
- Utworzenie z urządzeń QNAP samoreplikującego się środowiska backupowego w
- Instalacja Oprogramowania Backupowego wraz z konfiguracją na klastrach produkcyjnym i backupowym - Usługi wdrożeniowe:

    - Analiza środowiska – lokalizacji głównej serwerowni oraz lokalizacji zapasowej i przygotowanie projektu technicznego po konsultacjach z Zamawiającym.
    - Dostawa, instalacja, aktualizacja oprogramowania systemu wykonywania kopii zapasowych, monitorowania i analizowania monitorowania , konfiguracja całego środowiska zapewniająca poprawną pracę wszystkich elementów systemu infrastruktury uwzględniając wymagania Zamawiającego - i najlepsze praktyki i zalecenia producenta oprogramowania, a dokładnie:
        - Instalacja serwera systemu kopii zapasowych
        - Instalacja bazy danych systemu kopii zapasowych
        - konfiguracja dostępu do platform wirtualizacyjnych Zamawiającego
        - konfiguracja repozytorium przechowywania kopii zapasowych – udostępniona na urządzeniu QNAP posiadanym przez Zamawiającego
        - konfiguracja zadań backupowych – obejmująca do 20 wirtualnych maszyn – zarówno VMware vSphere jak i Hyper-V,
        - Instalacja i konfiguracja środowiska analitycznego i monitorującego działanie systemu wykonywania kopii bezpieczeństwa
        - przeprowadzenie pełnego backupu wszystkich maszyn wirtualnych i fizycznych

- dokonanie analizy działania całej infrastruktury backcupowej we wszystkich lokalizacjach
- w przypadku stwierdzenia możliwości wprowadzenia optymalizacji zadań – wdrożenie ich
- strojenie wydajnościowe rozwiązania

  Przygotowanie dokumentacji powykonawczej dokumentującej strukturę systemu, wszystkie kluczowe elementy, zawierającej schemat tworzenia zadań backupowych jak i procedurę ich testowania i odtwarzania produkcyjnego systemu z kopii zapasowej

- Instalacja i konfiguracja oprogramowania do zarządzania systemami serwerowymi oraz urządzeniami sieciowymi
- Wykonawca wdroży system kontroli dostępu do sieci LAN i WLAN za pomocą protokołu 802.1x wraz z integracją z Active Directory (konfiguracja przygotowana dla minimum 200 urządzeń)
- Wykonawca musi wykonać podział sieci na segmenty minimalnie:
  - VLAN Urząd Data
  - VLAN Urząd VOICE
  - VLAN WGKiK
  - VLAN Management
  - VLAN Wifi Urząd
  - VLAN Wifi Goście
  - VLAN CCTV
- Wykonanie testów działania zrekonfigurowanej sieci LAN
- Wykonanie testów działania zrekonfigurwanych usług WAN
- Przeprowadzenie szkolenia autorskiego dla wyznaczonych pracowników Referatu Informatyki wskazanych przez Zamawiającego. Szkolenie musi prezentować pełen zakres prac, rozwiązań ich budowy, architektury przyjętego rozwiązania, wykorzystanych procedur. Szkolenie w wymiarze minimum 20 godzin.
- Wykonanie i dostarczenie dokumentacji technicznej powykonawczej

Serwer RACK– 3 szt.

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Płyta główna	Płyta główna musi być zaprojektowana przez producenta serwera i trwale oznaczona jego znakiem firmowym na etapie produkcji. Płyta ma mieć możliwość instalacji dedykowanego przez producenta serwera znajdującego się w jego ofercie modułu GPU.	TAK	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach.	TAK	
Procesor	Zainstalowana moc procesora minimum 16 rdzeniowego klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 120 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji z zaoferowanym procesorem. Do oferty należy załączyć wydruk z wynikiem testu dla oferowanego modelu serwera.	TAK	
Pamięć RAM	Zainstalowane minimum 256 GB pamięci RAM RDIMM o częstotliwości pracy min. 3200MHz w kościach po 32GB każda. Płyta główna powinna obsługiwać do min. 2TB pamięci RAM. Na płycie głównej powinny znajdować się minimum 16 sloty przeznaczone dla pamięci w pełni dostępne. Opcjonalna obsługa pamięci NV DIMM. Powinny być możliwe min następujące ustawienia zabezpieczenia pamięci: SDDC, Memory Rank Sparing, Memory Mirror, LockStep, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling	TAK	
Dysk twardy	Zainstalowane minimum: 1 dysk twardy 2,5” o pojemności min. 480GB SSD SAS 12Gb/s, Hot-Swap przeznaczone do mieszanego obciążenia (Mix Use) o współczynniku 3DWPD, Możliwość instalacji łącznie min. 8 dysków twardych 2,5” SATA, SAS, NearLine SAS i SSD bez konieczności modyfikacji obudowy serwera. Wymagana Obsługa dysków typu SED i 4k.	TAK	
Kontroler dysków	Sprzętowy kontroler dyskowy, zapewniający obsługę dysków z prędkościami transferu 3, 6, 12 Gb/s, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10, 50, Wymagana obsługa dysków typu SED i 4k.	TAK	

Karta graficzna	Zintegrowana karta graficzna umożliwiająca wyświetlanie obrazu w rozdzielczości min. 1920x1200	TAK	
Sloty PCI-Express	min. 2szt x PCIe x16 nisko profilowe w tym min. 1 Gen4	TAK	
Porty wbudowane na płycie głównej	Min. 5 portów USB w tym min. 2x USB3.0 oraz 1x micro-usb dedykowany do karty zarządzającej, min 3 porty na przednim panelu Min. 3 porty RJ45 (w tym jeden dedykowany dla karty zarządzającej), Min. 2 porty VGA (1 na przednim panelu) Min. 1 port RS232	TAK	
Interfejsy sieciowe	Zainstalowane: 2 porty Ethernet Base-T działające z prędkością 1Gb/s 2 karty 2 portowe (każda) Ethernet Base-T z obsługą protokołu iSCSI działające z prędkością 10Gb/s	TAK	
Wewnętrzny redundantny moduł hypervisora	Zainstalowane minimum 2 identyczne nośniki flash M.2 o pojemności min. 480GB każdy dla hypervisora wirtualizacyjnego VMware wewnątrz serwera skonfigurowane w RAID 1 z poziomu BIOS serwera, nie zmniejszające minimalnej ilości wymaganych wnęk na dyski twarde Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 nośniki typu flash SD o pojemności min. 64GB. Rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.	TAK	
System diagnostyczny	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera. Panel musi umożliwiać wstępną parametryzację dostępu do serwera za pomocą przycisków funkcyjnych. Obudowa musi mieć możliwość wyposażenia interfejs umożliwiający dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (dostępnej na platformy Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.	TAK	
Zasilanie	Minimum 2 redundantne zasilacze o mocy 550W każdy, HotPlug, Hot – Swap	TAK	
Wentylatory	Minimum 6 redundantnych wentylatorów Hot-Plug, Hot – Swap,	TAK	

Napęd optyczny	Nie wymagany	TAK	
System operacyjny	Serwerowy System Operacyjny Microsoft Windows Server Standard 2019 – min 3x 16core lub równoważny zgodnie z warunkami równoważności opisanymi poniżej – pkt 3 (**wymagana ilość dla pojedynczego serwera**)	TAK	
Obudowa	Obudowa Rack o wysokości maksymalnej 1U z możliwością instalacji min. 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie Rack 19” i wysuwanie serwera do celów serwisowych wraz z organizatorem kabli. Obudowa ma posiadać dodatkowy, dedykowany przez producenta serwera, przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.	TAK	
Bezpieczeństwo	Zintegrowany trwale z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez serwer kluczami szyfrowania - TPM. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.	TAK	
System Zarządzania	Niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płytą główną posiadająca port RJ45 1Gb/s, posiadająca minimalną funkcjonalność: - podstawowe zarządzanie serwerem poprzez protokół IPMI 2.0, SNMP, VLAN tagging, Telnet, SSH - wbudowana diagnostyka - wbudowane narzędzia do instalacji systemów operacyjnych - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń - monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer - możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów - lokalna oraz zdalna konfiguracja serwera - zdalna instalacja systemów operacyjnych - wsparcie dla IPv4 i IPv6 - zapis zrzutu ekranu z ostatniej awarii - integracja z Active Directory - wirtualna konsola z dostępem do myszy i klawiatury - udostępnianie wirtualnej konsoli	TAK	

	- autentykacja poprzez publiczny klucz (dla SSH) - możliwość obsługi poprzez dwóch administratorów równocześnie - możliwość zarządzania poprzez bezpośrednie podłączenie kablem do dedykowanego złącza USB na froncie obudowy - możliwość podłączenia lokalnego poprzez złącze RS-232 - producent systemu musi posiadać dedykowane rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe. - wysyłanie do administratora powiadomienia e-mail o awarii lub zmianie konfiguracji sprzętowej - możliwość zablokowania konfiguracji oraz odnowienia oprogramowania karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty. - musi być zapewnioa możliwość monitorowania i zarządzania z jednej konsoli 20 serwerami fizycznymi w tym posiadanymi już przez Zamawiającego. Wymagana funkcjonalności karty zarządzającej rozszerzona o automatyczne przywracanie ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów z dedykowanej pamięci flash zainstalowanej (w tym kontrolera RAID, kart sieciowych, płyty głównej). Wymagana integracja dedykowanego oprogramowania producenta serwera z konsolą zarządzającą wymaganej platformy wirtualizacyjnej - Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH - Możliwość oskryptowywania procesu wykrywania urządzeń - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - Szczegółowy opis wykrytych systemów oraz ich komponentów - Możliwość eksportu raportu do CSV, HTML, XLS - Grupowanie urządzeń w oparciu o kryteria użytkownika		

	- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń - Szybki podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń - Integracja z service desk producenta dostarczonej platformy sprzętowej - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu - Kreator umożliwiający dostosowanie akcji dla wybranych alertów - Możliwość importu plików MIB - Przesyłanie alertów „as-is" do innych konsol firm trzecich - Możliwość definiowania ról administratorów - Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych - Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).		
Oświadczeni deklaracje	Certyfikat ISO9001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 50001 dla producenta sprzętu – dołączyć do oferty	TAK	

(załączyć do oferty)	Deklaracja zgodności CE – dołączyć do oferty Oferowany serwer musi znajdować się na liście Microsoft Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Oferowany serwer musi znajdować się na liscie Vmware Compatibility Guide i posiadać wsparcie dla wersji 6.5U3, 6.7U3, 7.0 oraz 7.0U1		
Gwarancja producenta na serwer	Minimum 5 lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta serwera. W przypadku awarii dysku twardego - uszkodzony dysk twardy pozostaje u Zamawiającego. Zamawiający w celu optymalizacji kosztów i utrzymania jednolitego wysokiego SLA usług serwisowych wymaga aby gwarancja była realizowana przez tą samą organizację która odpowiada za świadczenie usług dla posiadanego przez Zamawiającego sprzętu – serwerów Dell PowerEdge R730 Jeżeli serwer w standardzie posiada inną gwarancję należy podać odpowiedni pakiet rozszerzający gwarancję producenta serwera wraz z jego kodem/nazwą produktu. Firma serwisująca musi posiadać certyfikat ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające dołączyć do oferty. Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – dokumenty potwierdzające załączyć do oferty. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej urządzenia oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu serwera – w ofercie należy wskazać odpowiedni link strony.	TAK	

Macierz dyskowa - 1 szt.

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Dysk twardy	Zainstalowane: 5 dysków 2,5” Hot-Plug SSD SAS do intensywnego odczytu o pojemności 1,92TB SAS 12Gb/s, 10 dysków 2.5” Hot-Plug SAS 10k RPM o pojemności 2.4TB 8 dysków 12TB NLSAS 7.2k RPM 3,5” Hot-Plug, Musi być zapewniona możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 275 dysków i rozbudowy pojemności macierzy do 3PB. Macierz musi zapewniać możliwość mieszania typów dysków w obrębie zarówno macierzy oraz pojedynczej półki. Wymagane jest aby macierz obsługiwała dyski samoszyfrujące (SED) Typy obsługiwanych dysków: NL-SAS (7,2k RPM) 3,5": 4 TB, 8 TB, 12 TB, samoszyfrujące 12 TB, 16TB NL-SAS (7,2k RPM) 2,5": 2 TB, samoszyfrujące 2 TB SAS (10k RPM) 2,5": 1,2 TB, 1,8 TB, 2,4 TB, samoszyfrujące 2,4 TB SAS (15k RPM) 2,5": 900 GB, SSD: 480 GB, 960 GB, 1,92 TB, samoszyfrujące 1,92 TB, 3,84TB Dysk twarde/SSD: samoszyfrujące napędy z certyfikatem FIPS	TAK	
Kontroler dysków	Dwa kontrolery RAID pracujące w układzie active-active, Macierz musi udostępniać co najmniej 16GB pamięci cache opartej o pamięć DRAM z możliwością rozszerzenia cache odczytu o pamięć typu flash do min 4TB. Pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 3 doby w razie awarii. Backplane minimum SAS 12Gb/s	TAK	
Ciągłość pracy	Wymagana jest nieprzerwana, ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Kontrolery RAID macierzy muszą być redundantne, Hot-Swap; Zasilacze, wentylatory zarówno w macierzy jak i półkach dyskowych muszą być redundantne i Hot-Swap	TAK	
Wsparcie wirtualizacji	Macierz musi udostępniać dedykowane przez jej producenta rozszerzenia (plugin) do wykorzystywanego w infrastrukturze klienta oprogramowania	TAK	

	VMware vCenter dla zapewnienia lepszego, bezpośredniego zarządzania z poziomu konsoli vCenter, oraz dodatkowo plugin do VMware SRM		
Porty, interfejsy	Macierz musi udostępniać łącznie minimum osiem portów 10GbE Base-T iSCSI, 2 dedykowane porty zarządzające Dodatkowe półki dyskowe muszą być podłączane poprzez interfejs SAS 12Gb/s	TAK	
Wymagane funkcjonalności	Funkcjonalności wymagane – dostarczone razem z macierzą – dla pełnej maksymalnej pojemności macierzy (uwzględniając opcjonalną rozbudowę o maksymalną ilość półek dyskowych i dysków twardych): • Zarządzanie macierzą co najmniej poprzez przeglądarkę internetową, GUI oparte o HTML5 (nie dopuszcza się konieczności instalacji dedykowanych aplikacji zarządzających „tzw. gruby klient") • Macierz musi umożliwiać maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN'ów oraz 1024 kopii migawkowych na całą macierz. • Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji. • Macierz musi pozwalać na podłączenie bezpośrednie hostów – bez pośrednictwa sieci SAN • Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy wszystkimi wymaganymi typami dysków. • Macierz musi pozwalać na tworzenie wolumenów typu Thin • Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD. • Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym • Macierz musi zapewniać funknonalność wysyłania powiadamień mailem o awarii,		
Obsługiwane poziomy RAID	Macierz musi wspierać minimum następujące poziomy RAID: 0, 1, 10, 3, 5, 50, 6, rozproszony	TAK	

System diagnostyczny	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze, adresach MAC kart sieciowych, numerze serwisowym serwera, aktualnym zużyciu energii, nazwie serwera, modelu serwera. Panel musi umożliwiać wstępną parametryzację dostępu do serwera za pomocą przycisków funkcyjnych. Obudowa musi mieć możliwość wyposażenia interfejs umożliwiający dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej (dostępnej na platformy Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.	TAK	
Obudowa	Przeznaczona do instalacji w standardowej szafie RACK 19", macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5". Wraz z macierzą należy dostarczyć dodatkową półkę dyskową o wysokości 2U pozwalającą na instalację 12 dysków 3,5". Wymagane jest dostarczenie niezbędnych elementów montażowych (szyny Rack) oraz zabezpieczenia fizycznego zainstalowanych nośników w postaci dedykowanego przez producenta macierzy przedniego panelu chroniącego zainstalowane dyski zamykanego na klucz.	TAK	
Oświadczenia, certyfikaty, deklaracje (załączyć do oferty)	Certyfikat ISO9001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 50001 dla producenta sprzętu – dołączyć do oferty Deklaracja zgodności CE – dołączyć do oferty Oferowana macierz musi znajdować się na liście Microsoft Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012R2, systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Oferowany macierz musi znajdować się na liscie Vmware Compatibility Guide i posiadać wsparcie dla wersji 6.5U3, 6.7U3, 7.0 oraz 7.0U1 Oferowana maceirz musi mieć wsparcie dla dystrybucji systemu Linux co najmniej: Red Hat Enterprise Linux (RHEL) 6.9, 7.6 oraz 8.0 , SLES 12.3 oraz 15.0,	TAK	
Gwarancja producenta na macierz	Minimum 5 lat gwarancji producenta macierzy realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta macierzy.	TAK	

	W przypadku awarii dysku twardego - uszkodzony dysk twardy pozostaje u Zamawiającego. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i ich transportu Zamawiający w celu optymalizacji kosztów i utrzymania jednolitego wysokiego SLA usług serwisowych wymaga aby gwarancja była realizowana przez tą samą organizację która odpowiada za świadczenie usług dla posiadanego przez Zamawiającego sprzętu – serwerów Dell PowerEdge R730 Jeżeli w standardzie macierz posiada inną gwarancję niż wymagana należy w ofercie podać odpowiedni pakiet rozszerzający gwarancję producenta wraz z jego kodem/nazwą produktu pozwalający zweryfikować zgodność z wymaganiem. Firma serwisująca musi posiadać certyfikat ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające dołączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. A w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej Producent przejmie na siebie wszelkie zobowiązania związane z serwisem. – dokumenty potwierdzające załączyć do oferty. Musi istnieć możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer seryjny urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej urządzenia oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp na stronie producenta do najnowszych uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. W		

	ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy.		

Przełącznik sieciowy - 11 szt.

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w 2 redundantne zasilacze o mocy min 1600W każdy,	TAK	
Interfejsy sieciowe	Minimum 48 portów Multi GigabitEthernet w standardzie BaseT 10Mb/100Mb/1Gb/2.5Gb Minimum 4 zintegrowane porty 25Gb Ethernet SFP28, Minimum 2 porty 40Gb QSFP+ Wsparcie dla Half-Duplex (10Mb/100Mb) przynajmniej dla 30 portów Ethernet	TAK	
Wsparcie dla urządzeń PoE	Minimum połowa (24) portów przełącznika musi wspierać standard PoE dla urządzeń o poborze mocy 60W (802.3bt Type-3). Pozostałe porty muszą wspierać obciążenie do 30W.	TAK	
Ciągłość pracy	Przystosowanie do pracy w temperaturze 0-45 stopni Celcjusza	TAK	
Interfejsy zarządzające	Minimum 1 port USB typ A do konfiguracji przełącznika, 1 port Micro USB (typ B) 1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232. Dedykowany port ethernet do zarządzania typu Out-of-band	TAK	
Możliwości zarządzania	Obsługa protokołu sflow Obsługa SNMP v1/2/3 Zarządzanie przez interfejs WWW Obsługa Openflow 1.3 Obsługa skryptów Python Możliwość konfiguracji makr uproszczających zarządzanie systemem	TAK	

Praca w stosie	Możliwość połączenia w stos do 12 przełączników. Wydajność połączeń w stosie min. 160Gbps. Dopuszcza się wykorzystanie interfejsów Ethernet (min. 40Gbps) bądź dedykowanych	TAK	
Wydajność przełącznika	Minimum 32000 adresów MAC Przepustowość przełącznika min. 600Gbps, oraz min. 830Mpps Bufor pamięci dla pakietów minimum 4MB Obsługa min 8 kolejek QoS na port fizyczny		
Wbudowana pamięć	Pamięć RAM min. 4GB Pamięć flash min. 8GB		
Funkcjonalności warstwy L2	Obsługa minimum 4000 wirtualnych sieci VLAN Wsparcie dla agregacji LACP (802.3AX) Obsługa 128 grup LACP i 8 portów fizycznych per grupa Wsparcie la protokołu protekcji Ringu G.8032 Zgodność ze standardami wyspecyfikowanymi poniżej: 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP 802.1D Bridging, Spanning Tree, 802.1S Multiple Spanning Tree (MSTP) 802.1W Rapid Spanning Tree (RSTP) RSTP-Per VLAN 802.1v Protocol-based VLANs	TAK	
Funkcjonalności warstwy L2	Obsługa minimum 256 wpisów routingu IPv4, minimum 128 wpisów routingu IPv6 Obsługa protokołu routingu dynamicznego RIP1 oraz RIP2 Obsługa multicastów i protokołu IGMP v1/2/3		
Bezpieczeństwo	Obsługa 802.1x, Guest vlan i Mac Authentication Bypass Obsługa mechanizmu Private VLAN Obsługa technologii port mirroring oraz remote port mirroring Obsługa list kontroli dostępu opartych o adresy MAC i IP Obsługa min.100 list kontroli dostępu i 3000 reguł sumarycznie dla wszystkich list Obsługa czasowych list kontroli dostępu Obsługa mechanizmów DHCP Snooping oraz ARP Inspection i IP Source Guard Obsługa mechanizmu wykrywającego błąd na warstwie fizycznej typu UDLD		
Inne wymagane	Zgodność ze standardem ONIE – możliwość instalacji na przełączniku innego systemu operacyjnego zgodnego z tym standardem Wsparcie sprzętowe standardu VXLAN-Lite Przystosowanie do pracy w temperaturze 0-45 stopni Celcjusza		

Oświadczenia, certyfikaty, deklaracje (załączyć do oferty)	Certyfikat ISO9001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 50001 dla producenta sprzętu – dołączyć do oferty Deklaracja zgodności CE – dołączyć do oferty	TAK	
Gwarancja producenta na przełącznik	Minimum 5 lat gwarancji producenta przełącznika z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii dni robocze poprzez ogólnopolską linię telefoniczną producenta przełącznika, obejmując naprawę lub wymianę wszelkich komponentów wewnętrznych (wentylatorów, zasilaczy) Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i ich transportu Zamawiający w celu optymalizacji kosztów i utrzymania jednolitego wysokiego SLA usług serwisowych wymaga aby gwarancja była realizowana przez tą samą organizację która odpowiada za świadczenie usług dla posiadanego przez Zamawiającego sprzętu – serwerów Dell PowerEdge R730 Jeżeli w standardzie oferowany przełącznik posiada inną gwarancję niż wymagana należy w ofercie podać odpowiedni pakiet rozszerzający gwarancję producenta wraz z jego kodem/nazwą produktu pozwalający zweryfikować zgodność z wymaganiem. Firma serwisująca musi posiadać certyfikat ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające dołączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. A w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej Producent przejmie na siebie wszelkie zobowiązania związane z serwisem. – dokumenty potwierdzające załączyć do oferty. Musi istnieć możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer seryjny urządzenia, oraz pobieranie uaktualnień oprogramowania wewnętrznego nawet w przypadku	TAK	

	wygaśnięcia gwarancji. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej urządzenia oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp na stronie producenta do najnowszych uaktualnień oprogramowania wewnętrznego nawet w przypadku wygaśnięcia gwarancji macierzy. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy.		

Szafa serwerowa Rack 42U z wyposażeniem – 1 szt

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Obudowa	Szafa Rack 19”. Wysokość minimum 199 cm, głębokość minimum 125cm, szerokość minimum 80 cm. Minimalna głębokość montażowa 110cm. Drzwi przednie i tylne perforowane w min. 65%, zdejmowane, zamykane na klucz. Tylne dzwi muszą być dzielone 50/50. Boczne ściany dzielone, zdejmowane. Szafa powinna mieć możliwość fabrycznego łączenia z innymi szafami tego samego modelu. Szafa powinna być wyposażona w elementy stabilizujące. Kolor - czarny	TAK	
Funkcjonalność	Szafa powinna umożliwiać montaż urządzeń zgodnie ze standardem CEA-310E/ EIA-310-E - 482.6mm (19”). Pionowe belki nośne szafy powinny pozwalać na przesuwanie ich w ramach obudowy. Obciążenie statyczne szafy nie mniejsze niż 1200kg Obciążenie dynamiczne szafy minimum 750kg.	TAK	
PDU	Wraz z szafą należy dostarczyć 8szt modułów PDU jednofazowych w pełni zarządzanych i kompatybilnych z oprogramowaniem zarządzającym posiadanego przez Zamawiającego centralnego zasilacza UPS firmy Eaton PowerWare. Wysokość montażowa - 0U (309 32A 1fazowa) 20xC13 oraz 4xC19 Wymagane jest przedłożenie oświadczenia producenta UPS – firmy Eaton PowerWare, zaświadczające że zaproponowany model PDU jest w pełni kompatybilny z posiadanym zasilaczem UPS		
Wyposażenie dodatkowe	konsola LCD z KVM: Obudowa Rack o wysokości maks. 1U konsola LCD z KVM wraz z kompletem podwojonych wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie. W ramach tego samego rozwiązania montażowego musi znajdować się monitor min 19” wraz z klawiaturą w układzie US i touchpadem . Całość rozwiązania w pozycji zamkniętej nie może przekraczać 1U.	TAK	

	KVM powinien posiadać porty: - min. 16 wbudowanych portów umożliwiających podłączenie do serwerów (złącze RJ45) - min 1 port GbE Do KVM jednocześnie powinien móc podłączyć się zdalnie jeden użytkownik lokalnie oraz jeden użytkownik zdalnie Zarządzanie powinno się odbywać poprzez interfejs sieciowy Wspierane przeglądarki: Internet Explorer, Chrome, Firefox, Safari, Opera, Mozilla Wspierane standardy wyświetlania: Lokalnie i zdalnie obsługa obrazu w rozdzielczości do 1920x1200 W komplecie dostarczone kable do podłączenia serwerów z KVM w ilości min 16 sztuk (złącze USB-A + VGA – RJ45)		
Gwarancja	2 lata gwarancji producenta. Jeżeli produkt w standardzie posiada inną gwarancję należy podać odpowiedni pakiet rozszerzający gwarancję producenta wraz z jego kodem/nazwą produktu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta szafy	TAK	

Biblioteka taśmowa - 1 szt.

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Liczba slotów	Min. 32 w tym minimum pięć slotów we/wy, jeżeli licencjonowana jest liczba slotów - wymagane aktywowanie wszystkich slotów W komplecie należy dostarczyć min. 1 taśma czyszcząca oraz min. 10 taśm LTO-8 wraz z etykietami	TAK	
Napęd	1x LTO-8 z możliwością instalacji dodatkowych do min. 6 napędów LTO	TAK	
Ciągłość pracy	Wymagana jest nieprzerwana, ciągła praca urządzenia Zasilacze muszą być redundantne i Hot-Swap	TAK	
Porty, interfejsy	urządzenie musi udostępniać minimum 1 port SAS do połączenia z serwerem backupowym oraz min 1 port 1GbE Base-T dedykowany do zarządzania minimum 2 porty USB do diagnostyki i zarządzania. Dodatkowe opcjonalne napędy muszą być podłączane poprzez interfejs SAS	TAK	
Wymagane funkcjonalności	Funkcjonalności wymagane – dostarczone razem z biblioteką taśmową: • interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD • wyjmowane magazynki kieszeni na taśmy w celu łatwego zarządzania większą ilością taśm • wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja) • Obsługa SNMP, TLS1.2 oraz IP6 • Wsparcie dla technologii szyfrowania backupowanych danych – jeżeli funkcjonalność wymaga dodatkowej licencji należy ją umieścić w ofercie.		

	• Urządzenie musi zapewniać funkcjonalność wysyłania powiadomień mailem o awarii,		
Multipathing	biblioteka musi wspierać opcję wielościeżkowości - w przypadku zastosowania odpowiedniego napędu/ów		
Zarządzanie	Muszą być możliwe do utworzenia minimum 4 role dla administratorów z podziałem uprawnień na Administratora, Monitoring, Super użytkownika, Serwisowa.		
System diagnostyczny	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji stanie urządzenia. Panel musi umożliwiać wstępną parametryzację dostępu do urządzenia za pomocą przycisków funkcyjnych.	TAK	
Obudowa	Przeznaczona do instalacji w standardowej szafie RACK 19", biblioteka musi zajmować maksymalnie 3U. musi być wbudowany czytnik kodów kreskowych Wymagane jest dostarczenie niezbędnych elementów montażowych (szyny Rack) .	TAK	
Kontroler HBA	Wraz z biblioteką taśmową należy dostarczyć 1 kontroler HBA SAS 12Gb/s w postaci karty z dwoma zewnętrznymi portami SAS – karta musi być w pełni kompatybilna i objęta gwarancją producenta posiadanego serwera Dell PowerEdge R730		
Oświadczenia, certyfikaty, deklaracje (załączyć do oferty)	Certyfikat ISO9001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 50001 dla producenta sprzętu – dołączyć do oferty Deklaracja zgodności CE – dołączyć do oferty Oferowana biblioteka musi wspierać co najmniej systemy Microsoft Windows Server 2012R2, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Oferowana biblioteka musi mieć wsparcie dla dystrybucji systemu Linux co najmniej: Red Hat Enterprise Linux (RHEL) 6.9, 7.6 oraz 8.0 , SLES 12.3 oraz 15.0,	TAK	
Gwarancja producenta na bibliotekę taśmową	Minimum 5 lat gwarancji producenta biblioteki realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, zgłoszenia obsługiwane poprzez ogólnopolską linię telefoniczną producenta macierzy. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i ich transportu	TAK	

	Zamawiający w celu optymalizacji kosztów i utrzymania jednolitego wysokiego SLA usług serwisowych wymaga aby gwarancja była realizowana przez tą samą organizację która odpowiada za świadczenie usług dla posiadanego przez Zamawiającego sprzętu – serwerów Dell PowerEdge R730 Jeżeli w standardzie biblioteka posiada inną gwarancję niż wymagana należy w ofercie podać odpowiedni pakiet rozszerzający gwarancję producenta wraz z jego kodem/nazwą produktu pozwalający zweryfikować zgodność z wymaganiem. Firma serwisująca musi posiadać certyfikat ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta biblioteki – dokumenty potwierdzające dołączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. A w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej Producent przejmie na siebie wszelkie zobowiązania związane z serwisem. – dokumenty potwierdzające załączyć do oferty. Musi istnieć możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer seryjny urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej urządzenia oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp na stronie producenta do najnowszych uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta biblioteki.		

Przełącznik SAN - 10Gb/s - 2 szt.

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w 2 redundantne zasilacze	TAK	
Interfejsy sieciowe	Minimum - 28 x 10 Gigabit Ethernet RJ-45 - 2 x 100 Gigabit Ethernet QSFP28	TAK	
Ciągłość pracy	Przystosowanie do pracy w temperaturze 0-40 stopni Celcjusza	TAK	
Interfejsy zarządzające	1 port RJ45 do portu konsoli wraz z odpowiednim kablem RJ45-RS232. Dedykowany port ethernet do zarządzania typu Out-of-band	TAK	
Możliwości zarządzania	Obsługa protokołu sflow Obsługa SNMP v1/2/3 Zarządzanie przez interfejs WWW Obsługa Openflow 1.3 Obsługa skryptów Python Możliwość konfiguracji makr uproszczających zarządzanie systemem		
Wydajność przełącznika	• Musi obsługiwać ramki „Jumbo” o długości min. 9400 B. • Musi obsługiwać, co najmniej 4000 VLANów. • Pamięć dla co najmniej 160 000 adresów MAC.		
Wbudowana pamięć	Pamięć RAM min. 4GB		
Funkcjonalności warstwy L2	• Musi obsługiwać ramki „Jumbo” o długości min. 9400 B. • Musi obsługiwać, co najmniej 4000 VLANów. • Pamięć dla co najmniej 160 000 adresów MAC. • Musi obsługiwać co najmniej protokoły: STP, RSTP, PVST+, MSTP. • Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na	TAK	

	2 niezależnych opisywanych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń • Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG. • Musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow Control, funkcjonalność DCB oraz PFC i ECN. • Musi zapewniać sprzętowe wsparcie dla L3 VXLAN routing. • Musi być zgodny z następującymi standardami IEEE: • 802.1AB LLDP • TIA-1057 LLDP-MED • 802.1s MSTP • 802.1w RSTP • 802.3ab Gigabit Ethernet (1000Base-T) • 802.3ad Link Aggregation with LACP • 802.3ae 10 Gigabit Ethernet (10GBase-X) • 802.3ba 40 Gigabit Ethernet (40GBase-X) • 802.3z Gigabit Ethernet (1000BaseX) • 802.1D Bridging, STP • 802.1p L2 Prioritization • 802.1Q VLAN Tagging, Double VLAN Tagging, GVRP • 802.1Qbb PFC • 802.1Qaz ETS • 802.1s MSTP • 802.1w RSTP PVST+ • 802.1X Network Access Control • 802.3ab Gigabit Ethernet (1000BASE-T) or breakout • 802.3ac Frame Extensions for VLAN Tagging • 802.3ad Link Aggregation with LACP • 802.3ae 10 Gigabit Ethernet (10GBase-X) • 802.3ba 40 Gigabit Ethernet (40GBase- SR4, 40GBase-CR4, 40GBase-LR4, 100GBase-SR10, 100GBase-LR4, 100GBase-ER4) on optical ports • 802.3bj 100 Gigabit Ethernet • 802.3u Fast Ethernet (100Base-TX) na porcie zarządzania		

	• 802.3x Flow Control • 802.3z Gigabit Ethernet (1000Base-X) z adapterem QSA • ANSI/TIA-1057 LLDP-MED		
Funkcjonalności warstwy L3	• Musi obsługiwać protokoły dynamicznego routing dla IPv4 i dla IPv6: OSPF, BGP. • Musi obsługiwać protokół BFD, przynajmniej dla protokołu OSPF i OSFP v3. • Musi przechowywać minimum 200 000 wpisów rotingu IPv4 i minimum 160 000 wpisów routigu IPv6 • Musi wspierać mechanizm L3 ECMP Load Balancing. • Musi wspierać protokół redundancji VRRP • Wsparcie dla DHCP server i DHCP Relay • Obsługa Policy Based Routing. • Musi obsługiwać funkcjonalność VxLAN, Static VxLan, BGP eVPN oraz BGP eVPN Layer2 Vxlan gateway. • Musi obsługiwać poniższe standardy w zakresie protokołów routingu: • 791 IPv4 • 792 ICMP • 826 ARP • 1027 Proxy ARP • 1035 DNS (client) • 1042 Ethernet Transmission • 1191 Path MTU Discovery • 1305 NTPv4 • 1519 CIDR • 1812 Routers • 1858 IP Fragment Filtering • 2131 DHCP (server and relay) • 5798 VRRP • 3021 31-bit Prefixes • 3046 DHCP Option 82 (Relay) • 1812 Requirements for IPv4 Routers • 1918 Address Allocation for Private Internets • 2474 Diffserv Field in IPv4 and Ipv6 Headers		

	• 2596 Assured Forwarding PHB Group • 3195 Reliable Delivery for Syslog • 3246 Expedited Assured Forwarding • COPP: Control Plane Policing • Policy Based Routing • 2460 IPv6 • 2462 Stateless Address AutoConfig • 2463 ICMPv6 • 2464 Ethernet Transmission • 2675 Jumbo grams • 3587 Global Unicast Address Format • 4291 IPv6 Addressing • 2464 Transmission of IPv6 Packets over Ethernet Networks • 2711 IPv6 Router Alert Option • 4007 IPv6 Scoped Address Architecture • 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers • Dla protokołu OSPF • 1587 NSSA • 1745 OSPF/BGP interaction • 1765 OSPF Database overflow • 2154 MD5 • 2328 OSPFv2 • 2370 Opaque LSA • 3101 OSPF NSSA • Dla protokołu BGP • 1997 BGP Communities • 2385 MD5 • 2439 Route Flap Damping • 2796 Route Reflection • 2842 Capabilities • 2918 Route Refresh • 3065 Confederations • 4271 BGP-4 • 4360 Extended Communities • 4893 4-byte ASN • 5396 4-byte ASN Representation		

Mechanizmy bezpieczeństwa i QoS	**Musi wspierać następujące mechanizmy związane z zapewnieniem, jakości obsługi (QoS) w sieci:** • Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, vlan, wartość DSCP • Implementacja co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. • Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). • Implementacja mechanizmu Weighted Random Early Detection (WRED) • Obsługa IP Precedence i DSCP • Obsługa Control-Plane-Policing (ochrona systemu operacyjnego przed atakami DoS) **Musi wspierać następujące mechanizmy związane z zarządzaniem i zapewnieniem bezpieczeństwa w sieci:** • Co najmniej 3 poziomy dostępu administracyjnego przez konsole: • Autoryzacja użytkowników/portów w oparciu o 802.1x • Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6 **Musi wspierać następujące mechanizmy zarządzania** • Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2 • Obsługa monitorowania ruchu na porcie (Port Monitoring), ACL-Based Monitoring oraz RSPAN • Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony 10/100/1000BaseT • Plik konfiguracyjny urządzenia musi być możliwy do edycji ‘off-line’, tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian.		

	• Wsparcie dla mechanizmu Beacon LED control – włączenie diody danego interfejsu celem identyfikacji • Urządzenie musi posiadać funkcjonalność automatycznej instalacji oprogramowania poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware), w trakcie pierwszego podłączenia do sieci Ethernet • Urządzenie musi mieć możliwość utworzenia skryptów systemu linux oraz uruchomienia skryptów utworzonych w języku Python oraz Python oraz umożliwiać jego konfigurację przez narzędzia Ansible, Chef i Puppet		
Inne wymagane	Zgodność ze standardem ONIE – możliwość instalacji na przełączniku innego systemu operacyjnego zgodnego z tym standardem Wsparcie sprzętowe standardu VXLAN-Lite		
Oświadczenia, certyfikaty, deklaracje (załączyć do oferty)	Certyfikat ISO9001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 14001 dla producenta sprzętu – dołączyć do oferty Certyfikat ISO 50001 dla producenta sprzętu – dołączyć do oferty Deklaracja zgodności CE – dołączyć do oferty	TAK	
Gwarancja producenta na przełącznik	Minimum 5 lat gwarancji producenta przełącznika z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii dni robocze poprzez ogólnopolską linię telefoniczną producenta przełącznika, obejmując naprawę lub wymianę wszelkich komponentów wewnętrznych (wentylatorów, zasilaczy) Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i ich transportu Zamawiający w celu optymalizacji kosztów i utrzymania jednolitego wysokiego SLA usług serwisowych wymaga aby gwarancja była realizowana przez tą samą organizację która odpowiada za świadczenie usług dla posiadanego przez Zamawiającego sprzętu – serwerów Dell PowerEdge R730 Jeżeli w standardzie oferowany przełącznik posiada inną gwarancję niż wymagana należy w ofercie podać odpowiedni pakiet rozszerzający gwarancję producenta wraz z jego kodem/nazwą produktu pozwalający zweryfikować zgodność z wymaganiem.	TAK	

	Firma serwisująca musi posiadać certyfikat ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające dołączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. A w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej Producent przejmie na siebie wszelkie zobowiązania związane z serwisem. – dokumenty potwierdzające załączyć do oferty. Musi istnieć możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer seryjny urządzenia, oraz pobieranie uaktualnień oprogramowania wewnętrznego nawet w przypadku wygaśnięcia gwarancji. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej urządzenia oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp na stronie producenta do najnowszych uaktualnień oprogramowania wewnętrznego nawet w przypadku wygaśnięcia gwarancji macierzy. W ofercie wymagane jest wskazanie odpowiedniego linku do strony internetowej producenta macierzy.		

System Kontroli Dostępu (obsługa 2 przejść).

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Kontroler (1 szt.)	Kontroler musi umożliwiać obsługę 2 przejść kontrolowanych dwustronnie Oferować rejestrację zdarzeń dla celów RCP oraz integrację z systemem alarmowym.	TAK	

Dane Techniczne	8192 identyfikatorów - 8 nośników (karta, PIN, odcisk itp.) w ramach jednego identyfikatora - 32 uprawnienia na identyfikator - 16 przejść dwustronnych (drzwi) - 32 punkty logowania - 64 terminale dostępu (czytniki) - 16 stref dostępu - 16 stref alarmowych - 32 węzły automatyki - 512 uprawnień - 64 reguły w ramach jednego uprawnienia - 64 tryby RCP - 16 trybów logowania - 4 kroki identyfikacji w ramach jednego trybu logowania - 64 linie wejściowe - 64 linie wyjściowe - 64 klawisze funkcyjne - 32 komendy sterujące - wielofunkcyjne parametryczne linie wejściowe - wielofunkcyjne linie wyjściowe z obsługą priorytetów oraz sposobów modulacji - blokada wielokrotnego wejścia z czasowym resetem (Timed Anti-passback) - 32 kalendarze - 99 przedziałów czasowych w ramach kalendarza - 250 harmonogramów czasowych - 40 przedziałów czasowych w ramach jednego harmonogramu - 16 wyjątków w ramach jednego harmonogramu - bezpośrednia obsługa 16 czytników serii MCT (interfejs RS485) - możliwość podłączenia 4 czytników serii PRT do płyty głównej kontrolera - możliwość podłączenia 4 czytników typu Wiegand do płyty głównej kontrolera - obsługa czytników PRT i Wiegand za pośrednictwem interfejsów magistralowych MCX - 8 parametrycznych linii wejściowych na płycie kontrolera - 8 wyjść tranzystorowych na płycie kontrolera - 2 wyjścia przekaźnikowe na płycie kontrolera - bufor 8 milionów zdarzeń na wymiennej karcie pamięci	TAK	

	- zasilanie DC lub AC - ładowanie i monitorowanie baterii rezerwowej - interfejs CLK/DTA - 2 interfejsy RS485 - interfejs komunikacyjny Ethernet - szyfrowana transmisja danych - szybka konfiguracja (poniżej 1 minuty) - przesłanie ustawień w tle bez zatrzymywania bieżącej pracy systemu - wbudowany zasilacz impulsowy z wyjściem 1.0A/12VDC - aktualizacja oprogramowania wbudowanego (firmware) - możliwość migracji płyty głównej do wyższych wersji przez zakup dodatkowej licencji		
Ekspander we/wy 2 przejścia - 1 sztuka	- dystrybucja zasilania do 2 przejść - dystrybucja magistrali komunikacyjnej - 4 wejść EOL/2EOL - 4 wyjść 12 V/1 A - 5 wyjścia zasilania 12 V/1 A - 5 wyjścia zasilania 12 V/0,2 A - interfejs komunikacyjny RS485 do kontrolera dostępu - zabezpieczenie przed głębokim rozładowaniem akumulatora - raportowanie stanów zasilania do kontrolera dostępu - ładowanie akumulatora prądem 0,3 A, 0,6 A lub 0,9 A - zasilanie z zewnętrznego zasilacza 13,8 VDC/5 A		
Czytnik zbliżeniowy w standardzie MIFARE. (4 sztuki)	Częstotliwość pracy 13,56 MHz, - Pobór prądu 20mA przy 24VDC, max 60mA, - Obsługiwane standardy MIFARE® DESFire: UID, MIFARE® Classic: UID, MIFARE® Ultralight UID, MIFARE® Plus UID, MIFARE® SmartMX (MIFARE® Classic emulation mode) UID, NFC (UID), Mifare Classic 7 Byte UID, - Wymiary obudowy 141 x 43 x 19 mm, - Kolor Czarny, - Stopień ochrony wersja z przewodem/konektorem IP67/IP54 - Wyjścia 2xFET (do tampera oraz uniwersalne) - Interfejsy kompatybilne z kontrolerem/ekspanderem. - Kompatybilność elektromagnetyczna zgodnie z normą EN300330 - LED 3-kolorowa możliwa do programowania	TAK	

	- Buzzer - (możliwość programowania trybu pracy) - Tamper optyczny - programowalny - Opóźnienie ponownego odczytu karty - programowalne w zakresie do 99 sek - Temperatura pracy -40 °C - +55 °C		
Elementy wykonawcze	W drzwiach serwerownia oraz PPD należy zainstalować elektrozaczep oraz zworę elektromagnetyczną z czujnikiem otwarcia drzwi.	TAK	

Centrala Alarmowa

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Dane Techniczne Centrala	Obsługa do 230 urządzeń (w tym 120 bezprzewodowych), · 600 użytkowników · 15 stref · 128 programowalnych wyjść PG (w tym 32 bezprzewodowe) · 64 niezależnych wydarzeń kalendarzowych · Raporty SMS do 50 użytkowników · Raporty głosowe do 15 użytkowników · możliwość ustawienia 5 SMA · 5 wybieralnych protokołów do SMA · poziom bezpieczeństwa 2/klasa środowiskowa II (zgodnie z EN 50131-1) · Komunikator LAN - Interfejs ethernetowy, 10/100BASE-T Pasywne czujki podczerwieni PIR · Zasilanie 12 V z magistrali centrali · Zużycie energii elektrycznej w trybie awaryjnym: 5 mA · Zużycie energii elektrycznej dla wybranych przewodów 5 mA · Zalecana wysokość montażu: 2 m nad poziomem podłogi · Kąt / obszar detekcji 90°/12 m, 90° / 7 m (odporność na zwierzęta domowe) · Klasyfikacja EN 50131-1 wyd. 2+A1+A2, EN 50131-2-2 · Środowisko zgodne z EN 50131-1 II, wewnętrzne, ogólne · Spełnia wymogi EN 50130-4 wyd. 2+A1, EN 55032, EN 50581 Czujka magnetyczna otwarcia (kontaktron) · Zasilanie: z magistrali BUS systemu 12 V (9 - 15 V) · Pobór prądu w czuwaniu: 5 mA · Stopień ochrony 2, zgodnie z normami EN 50131-1 · Zgodny z standardami: EN 50130-4, EN 55022 · Czujka magnetyczna otwarcia (kontaktron) garażowy	TAK	

	· Montaż nawierzchniowy · Szczelina 65mm · Wyjście alarmowe NC · Obudowa metalowa · Osłona przewodu metalowa · Zgodność z EN50131GRADE2 Sygnalizator optyczno – akustyczny · Zasilanie: 10 do 17 V DC · Zużycie prądu < 50 mA / 12 V · Podtrzymanie zasilania: bateria NiCd 4.8 V / 1800 mAh (żywotność ok. 3 lata) · Poziom dźwięku: 110 dB /1 m · Timer syreny: 5 minut · Timer błysku: 30 minut · Rezystancja tampera< 70 Ω · Stopień ochrony: 2, EN 50131 Czujki temp/zalania dodac		
Czujka PIR (4 sztuki)	· Zasilanie 12 V z magistrali centrali · Zużycie energii elektrycznej w trybie awaryjnym: 5 mA · Zużycie energii elektrycznej dla wybranych przewodów 5 mA · Zalecana wysokość montażu: 2 m nad poziomem podłogi · Kąt / obszar detekcji 90°/12 m, 90° / 7 m (odporność na zwierzęta domowe) · Klasyfikacja EN 50131-1 wyd. 2+A1+A2, EN 50131-2-2 · Środowisko zgodne z EN 50131-1 II, wewnętrzne, ogólne · Spełnia wymogi EN 50130-4 wyd. 2+A1, EN 55032, EN 50581	TAK	
Czujnik zalania (4 sztuki)	· Zasilanie: z magistrali BUS systemu 12 V (9 - 15 V) · Pobór prądu w czuwaniu: 5 mA · Stopień ochrony 2, zgodnie z normami EN 50131-1 · Zgodny z standardami: EN 50130-4, EN 55022	TAK	
Czujnik temperatury i dymu (2 sztuki)	- Zasilanie: z magistrali BUS systemu 12 V (9 - 15 V) oraz bateryjne - Zgodny z standardami: EN 54-25, ETSI EN 300 220, EN 60950-1, EN 50130-4 i EN 55022 - Czułość temperaturowa: klasa A1	TAK	

	-Czułość dymowa: m = 0.11 – 0,13 dB/m		

Kamera CCTV – 4 szt.

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Standard	Kamera IP w standardzie TCP/IP	TAK	
Przetwornik	1 / 2.7” Progressive Scan CMOS	TAK	
Matryca	Min. 4 Mpix	TAK	
Obiektyw	2.8mm	TAK	
Kąt widzenia	Min. 105’	TAK	
Oświetlacz IR	Tak, zasięg min. 10 metrów	TAK	
Dodatkowe parametry	Kompresja obrazu H.265 Interfejs 100 Base-T Zasilanie POE Wbudowany Web Server Obudowa Dome z uchwytem sufitowym Kolor jasny/biały.	TAK	
Oprogramowanie VMS	Wraz z kamerami wymagane jest dostarczenie oprogramowania klasy VMS (dla minimum 8 kamer). Musi umożliwiać pracę nieograniczonej ilości użytkowników. Musi wspierać integrację z posiadaną przez zamawiającego usługą Active Directory z uwzględnieniem SSO za pomocą protokołu Kerberos. Oprogramowanie VMS musi komunikować się w standardzie h265. Kompatybilność z systemem operacyjnym Windows Server 2019 oraz Windows 10 Wraz z oprogramowaniem należy dostarczyć jedną licencję systemu operacyjnego Windows 10.	TAK	

System Kopii Zapasowych

Warunek graniczny/parametr	Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1	2	3
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. TCO rozwiązania Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków	**TAK**	

Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych. 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. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time) Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej re-instalacji Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.		

Wymagania RPO Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej Oprogramowanie musi 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 Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn Oprogramowanie musi posiadać wsparcie dla NDMP Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.		

Oprogramowanie musi 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. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing) Wymagania RTO Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) Oprogramowanie musi 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 Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2. Oprogramowanie musi 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		

Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: **Linux** ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs **BSD** UFS, UFS2 **Solaris** ZFS, UFS **Mac** HFS, HFS+ **Windows** NTFS, FAT, FAT32, ReFS **Novell OES** NSS Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. Oprogramowanie musi 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. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"), Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN		

Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN Funkcjonalność ograniczenia ryzyka Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. Monitoring System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.x oraz 6.x – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. System musi mieć status „VMware Ready" i być przetestowany i certyfikowany przez VMware System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter		

System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 8.x i 9.x Raportowanie System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.x oraz 6.x vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. System musi być certyfikowany przez VMware i posiadać status „VMware Ready”		

System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie Warunki i sposób udzielenia licencji Wymagania ogólne: dostarczona licencja na oprogramowanie spełniające powyższe wymagania musi posiadać możliwość swobodnego przeniesienia na dowolny podmiot wymieniony w umowie i dowolne wystąpienie - serwer zarówno fizyczny jak wirtualny jak również stacje klienckie będące w posiadaniu Zamawiającego (bez ograniczeń licencji OEM). Licencje dostępne w modelu licencjonowania na fizyczny procesor – minimum 6 szt. (nielimitowana ilość rdzeni procesora) w ramach jednego środowiska oraz konsoli		

zarządzającej i monitorującej środowisko Zamawiającego. Instancja wystąpienia musi zapewniać dowolność wykorzystania dla Zamawiającego pomiędzy serwerami fizycznymi, wirtualnymi a stacjami klienckimi w ramach zamawianej ilości. Wsparcie producenta oprogramowania realizowany w okresie 5 lat od nabycia licencji **Wymiar usługi: min. 60 miesięcy od dnia dostarczenia licencji** **Wymagania minimalne dla wsparcia:** Usługa wsparcia gwarancyjnego oraz subskrypcji dla oferowanego oprogramowania musi być świadczona na każdym etapie procesowania zgłoszenia przez producenta oprogramowania będącego licencjodawcą oprogramowania (wykluczona usługa serwisu realizowana przez firmy posiadające status partnera OEM). Zamawiający definiuje etapy świadczenia wsparcia/procesowania zgłoszenia serwisowego na: L1 – przyjęcie zgłoszenia, L2 – analiza i rekomendacje zmian, L3 – przygotowanie poprawek do oprogramowania. Oferowana usługa musi zapewniać ciągłość i poufność komunikacji na poszczególnych etapach procesowania zgłoszenia. Nie dopuszcza się procesowania zgłoszeń serwisowych przez firmy trzecie lub w systemach informatycznych nie zarządzanych przez producenta oprogramowania. Usługa wsparcia gwarancyjnego musi umożliwiać zgłaszanie problemów dni robocze Opis oferowanej usługi wsparcia musi być dostępny na oficjalnej stronie internetowej producenta oprogramowania.		

System Monitoringu Urządzeń Sieciowych

Warunek graniczny/parametr		Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1		2	3
Licencje	System powinien zarządzanie min. 25 urządzeniami, przy czym powinna istnieć możliwość stopniowej migracji do 2000 urządzeń z wykorzystaniem licencji na okres 3 lat	**TAK**	
System Operacyjny	Musi wspierać instalacje na następujących systemach operacyjnych: min. RedHat / Centos / Microsoft / Vmware		
Przeglądarki	Musi wspierać przeglądarki min. wersje Chrome/Safari/Firefox/Internet Explorer		
Obsługiwane urządzenia	• Przełączniki klasy datacenter, klasy dostępowej L2 i L3 • Oferowane punkty dostępowe		
Obsługiwane urządzenia innych producentów	Musi umożliwiać minimum obsługę 5 różnych producentów urządzeń sieciowych, które są ujęte w raportach Gartnera		
Funkcje NMS	Musi wspierać dostęp w oparciu o przeglądarkę		
	Musi funkcjonować w oparciu o następujące minimalne wymagania hardware: 8GB RAM, dual core CPU, disk 200GB		
	Oferowany NMS powinien umożliwiać skalowanie do zarządzania do 2000 urządzeń Musi raportować informacje o stanie gwarancji/wsparcia serwisowego dla dostarczonych przełączników w oparciu o informacje uzyskane prze połączenie do serwera producenta		
	Powinien zapewniać pojedynczy panel zarządzania zarówno dla sieci LAN i i WLAN Musi mieć możliwość automatycznej konfiguracji protokołu sflow na przełącznikach i pełnić rolę kolektora danych protokołu sflow		

	Musi umożliwiać wyszukiwanie urządzeń sieciowych oraz prezentacje ich szczegółowych danych dotyczących ich funkcjonalności oraz szczegółów połączenia Musi umożliwiać tworzenie szczegółowych profili wyszukiwania oraz możliwość automatycznej konfigracji protokołu SNMP na urządzeniach podczas procesu wyszukiwania		
	Musi umożliwiać prezentacje graficznej i fizycznej topologii map wszystkich zarządzanych urządzeń		
	Musi umożliwiać grupowanie urządzeń w oparciu o model, lokalizacje, number seryjny, asset tag, service tag, MAC, FW i SW		
	Musi zapewniać modyfikacje ustawień oraz oprogramowania dla wybranych wielu urządzeń jednocześnie		
	Musi zapewniać planowanie w określonym czasie zmiany konfiguracji urządzeń		
	Musi zapewniać monitorowanie stanu i wydajności sieci oraz poszczególnych urządzeń		
	Musi umożliwiać kreowanie tzw. Dashbord'ów zawierających informacje nt. zdarzeń sieciowych, wzorców ruchu sieciowego oraz trendów		
	Musi umożliwiać proaktywne monitorowanie problemów sieciowych, automatyczne zmiany konfiguracyjne dla wielu urządzeń		
	NMS musi umożliwiać audyt konfiguracji w celu śledzenia i naprawy problemów sieciowych		
	Musi zapewniać gromadzenie danych dotyczących analizy przepływów sieciowych w oparciu o dedykowane protokoły sieciowe dla zapewnienia optymalizacji konfiguracji wydajności sieci		
Funkcjonalność dodatkowe	Zewnętrzna konsola zarządzająca pozwalająca na zarządzanie wszystkimi urządzeniami za pomocą dedykowanego GUI		
	Konsola musi mieć następujące możliwości:		
	- Rozpoznawania urządzeń działających w sieci,		
	- zautomatyzowany proces upgrade’u oprogramowania na grupy urządzeń		
	- granularny dostęp administratorski z przypisanymi:		
	a) Rolami		
	b) Segmentami sieci, do których uzyskuje się dostęp		

	- tworzenia szablonów konfiguracji dla urządzeń podobnego typu		
	- monitorowania urządzeń i obsługa zdarzeń w sieci		
	- tworzenie raportów historycznych oraz czasu rzeczywistego z informacjami nt.: lokalizacji, numeru seryjnego, asset tag, service tag, MAC, FW i SW		
	- tworzenie raportów audytowych ze śledzeniem zmian w konfiguracji urządzeń		
	- wsparcie tzw. Multivendor, czyli możliwość zarządzania z wykorzystaniem SNMP innymi urządzeniami sieciowymi		
	Wsparcie dla autentykacji RADIUS, LDAP/AD i CAS		
	Musi istnieć możliwość delegowania zadań dla administratorów systemu		
	Musi istnieć możliwość tworzenia profili urządzenia wraz z danymi uwierzytelniającymi umożliwiającymi dostęp do różnych sposobów zarządzania (min. CLI, syslog, SNMP).		
	Musi istnieć możliwość z poziomu GUI systemu uzyskania dostępu bezpośrednio do konsoli CLI urządzenia z wykorzystaniem danych zawartych w profilach urządzeń		
	Musi istnieć możliwość implementacji w trybie wysokiej dostępności również poza mechanizmami środowiska wirtualnego		
Gwarancja	Gwarancja na całość rozwiązania: od tego samego Dostawcy.		
	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.		

Serwerowy System Operacyjny – 13 szt.

Warunek graniczny/parametr	Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1	**2**	**3**
Licencja na 16 rdzeni procesora		

Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu,		

b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. Login i hasło,		

b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. 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.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. 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: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,		

ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6),		

k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).		

28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.		
Do systemów operacyjnych należy dołączyć wymagane licencje Device CAL w ilości 200 szt	TAK	
Do systemów operacyjnych należy dołączyć wymagane licencje terminalowe RDS DevCAL w ilości 20szt.	TAK	

Oprogramowanie Serwera Bazodanowego

Warunek graniczny/parametr	Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1	2	3
System bazodanowy (SBD) licencjonowany w trybie Serwer + licencje dostępowe CAL dla użytkowników w liczbie 30 szt		
1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. 2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania. 3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem. 4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania). 6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych.		

7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech: - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD), - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach, 8. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych. 9. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych. 10. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory. 11. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. 12. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność		

rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń: - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system), - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur), - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy). 13. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci. 14. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji. 15. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi: - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli, - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD, - udostępniać język zapytań do struktur XML, - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML), - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.		

16. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności: - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów, - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp., - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD, - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.). 17. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania. 18. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny. 19. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania. 20. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.		

21. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera. 22. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.: - mechanizm debuggowania tworzonego rozwiązania, - mechanizm stawiania „pułapek” (breakpoints), - mechanizm logowania do pliku wykonywanych przez transformację operacji, - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu), - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo) - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli), - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach), - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać		

uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego, - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych. 23. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina. 24. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail). 25. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki). 26. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych. 27. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta). 28. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series),		

drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli. 29. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. 30. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać: - raporty parametryzowane, - cache raportów (generacja raportów bez dostępu do źródła danych), - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów), - współdzielenie predefiniowanych zapytań do źródeł danych, - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File), - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport, - możliwość wizualizacji wskaźników KPI, - możliwość wizualizacji danych w postaci obiektów sparkline. 31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services). 32. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w		

formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach. 33. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów. 34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja). 35. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT. 36. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD. 37. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań. 38. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).		

Platforma Wirtualizacja

Warunek graniczny/parametr	Warunek Graniczny	Parametry oferowane lub opis potwierdzający warunek graniczny (podać)
1	2	3
1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych 2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 3. Pojedynczy klaster może się skalować do 6 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. 4. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12 TB pamięci fizycznej RAM. 5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych. 6. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. 7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM. 8. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. 9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. 10. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 11. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 12. 13. Rozwiązanie musi 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. 14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. 15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 16. 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 HTML5. 17. 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. 18. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 20. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory. 21. 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. 22. 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. 23. 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. 24. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).		

25. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra 3 serwerów fizycznych. 26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy 3 serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. 27. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) dla klastra 3 serwerów , 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.		
Usługa wsparcia gwarancyjnego oraz subskrypcji dla oferowanego oprogramowania musi trwać minimum 5 lat od daty udzielenia licencji Zamawiający definiuje etapy świadczenia wsparcia/procesowania zgłoszenia serwisowego na: L1 – przyjęcie zgłoszenia, L2 – analiza i rekomendacje zmian, L3 – przygotowanie poprawek do oprogramowania. Opis oferowanej usługi wsparcia musi być dostępny na oficjalnej stronie internetowej producenta oprogramowania. **Usługa musi zapewnić:** • nieograniczona ilość zgłoszeń serwisowych • wsparcie zdalne przez pracownika serwisu producenta oprogramowania • dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy, forum internetowe producenta oprogramowania • gwarancję poufności w zarządzaniu przekazanymi informacjami (usługa świadczona bez możliwości i wymogu przesyłania logów oraz informacji o zgłoszeniach serwisowych poza system procesowania zgłoszeń zarządzany i administrowany przez producenta oprogramowania) • dostęp do poprawek i uaktualnień oprogramowania objętego usługą wsparcia • dostęp do portalu www producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, założenie zgłoszenia awarii u producenta, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji oprogramowania • dostęp do rejestru licencji (dostępnego przez portal www producenta oprogramowania) Centralny rejestr licencji musi udostępniać założenie i wysłanie do producenta zgłoszeń przeniesienia licencji na inny podmiot oraz zgłoszeń serwisowych kierowanych do producenta oprogramowania		

• czas odpowiedzi ze strony producenta oprogramowania dla zgłoszeń typu Critical (Severity 1) 4 godziny • czas odpowiedzi ze strony producenta oprogramowania dla zgłoszeń typu Major (Severity 2) 8 godziny roboczych • czas odpowiedzi ze strony producenta oprogramowania dla zgłoszeń typu Minor (Severity 3) 12 godziny roboczych		