**Opis przedmiotu zamówienia**

1. Przedmiotem postępowania jest dostawa infrastruktury teleinformatycznej. Obejmie ona sprzęt i oprogramowanie, instalację i wdrożenie.
2. Zamawiający, w każdym wypadku posłużenia się jednoznaczną nazwą produktu, dopuszcza produkty równoważne zgodne z wymaganiami opisanymi w s.i.w.z.
3. Wymagania techniczne opisane w s.i.w.z. wynikają z wymagań i specyfikacji produktu przedstawionego przez Wykonawcę rozstrzygniętego postępowania na dostawę pod nazwą „Zaprojektowanie, dostawa, konfiguracja i wdrożenie systemu biletu elektronicznego komunikacji aglomeracyjnej wraz z usługą wsparcia przez okres 48 miesięcy” numer sprawy DZ.381.UE-1/19, które będzie zainstalowane i wdrożone na dostarczonej w niniejszym postępowaniu infrastrukturze teleinformatycznej. Przedmiot dostawy został opisany w sposób wynikający z wymagań technicznych dla zakupionego systemu.
4. Specyfikacja techniczna dostarczanych w ramach niniejszego postępowania produktów- podział na 5 części:
5. **Część I**

Dostarczone w ramach części I poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:

* 1. Wszystkie oferowane urządzenia muszą być fabrycznie nowe (na dzień dostawy urządzenia nie mogą być starsze niż 6 miesięcy od daty produkcji oraz nie mogą być używane).
  2. Oferowany sprzęt musi pochodzić z produkcji seryjnej.
  3. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO9001:2000 lub normą równoważną. Zgodne z prawem obowiązującym w Unii Europejskiej dostarczone elementy infrastruktury muszą spełniać wytyczne dyrektywy CE (Conformité Européenne) i muszą być oznaczone znakiem CE.
  4. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
  5. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
  6. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: wkładek optycznych, kabli zasilających, kabli FC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
  7. Na dzień złożenia oferty oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
  8. Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji(na programowanie) Zamawiającemu lub przeniesie na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.

1. **Serwer typ 1 – 2 szt.**

Wymagana specyfikacja serwera.

* 1. Obudowa typu RACK 19”, maksimum 2U dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack, wraz z organizerem kabli.
  2. Płyta główna minimum dwuprocesorowa, z możliwością instalacji procesorów 28-rdzeniowych. Minimum 12 alokacji na dyski 2,5” SATA Hot – Plug. możliwość instalacji dysków SATA, SSD, SAS.
  3. Płyta główna jest obsługiwana przez wbudowany Chipset realizujący funkcję PCIe Uplink x16 (lub o wyższej krotności), umożliwiającą wykorzystanie wielu dodatkowych linii PCIe prowadzących do kontrolera płyty w celu zapewnienia wysokiej przepustowości I/O
  4. Złącza minimum – 6 aktywnych złącz PCI Express generacji 3 w tym: 3 fizyczne złącza o prędkości x16 oraz 3 fizyczne złącza o prędkości x8.
  5. Minimum 24 gniazda z możliwością zainstalowania minimum 3TB pamięci RAM.
  6. Dwa procesory minimum 24-rdzeniowe o architekturze x86\_64, osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 160 pkt (wynik dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html. Wykonawca załączy do oferty wydruk z wyżej wymienionej strony bez jej tłumaczenia na język polski, podpisany za zgodność z oryginałem przez Wykonawcę. W przypadku braku wyników dla oferowanego procesora oferent zobowiązany jest dołączyć oświadczenie producenta serwera, w którym opierając się na wynikach dostępnych dla innego procesora tego samego typu i tego samego producenta wykaże, iż oferowany procesor spełnia wymagania minimalne.
  7. Zainstalowana pamięć RAM min. 256 GB typu RDIMM lub LRDIMM o przepustowości min. 2666 MT/s. Pojedynczy moduł pamięci o pojemności min. 64 GB.
  8. Zainstalowane minimum: 4 dyski SAS 12G 600GB 10K 512n HOT PLUG. Dyski skonfigurowane w RAID 5.
  9. Zainstalowane minimum: 4 interfejsy LAN 1Gbit Base-T (w tym mini. 2 interfejsy ze wsparciem iSCSI oraz PXE boot), 4 interfejsy LAN 10Gbit MMF LC (z modułami SFP+ SR), interfejsy FC 2x 16Gb (z modułami SFP+ SWL).
  10. Zainstalowany kontroler RAID dla wewnętrznych dysków z 4 GB pamięci cache i podtrzymywaniem typu flash obsługujący poziomy RAID: 0,1,5,6. Kontroler RAID zainstalowany w serwerze musi obsługiwać 16 dysków (wbudowane złącza: 4x Mini-SAS HD x4) bez konieczności instalacji dodatkowych elementów (nie jest dopuszczalne stosowanie ekspanderów i dwóch kontrolerów).
  11. Zintegrowana karta graficzna ze złączem VGA, wbudowane w obudowę min. 1 port USB na panelu przednim, min. 1 port USB wewnętrzny ( lub rozwiązanie oparte na adapterze obsługującym dyski SSD M.2 w trybie RAID 1) min. 2 porty USB 3.0 dostępne z tyłu serwera.
  12. Zainstalowana i aktywna funkcja zdalnego zarządzania (konsoli) umożliwiająca: włączenie, wyłączenie, restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS), przejęcie zdalnej konsoli graficznej i podłączenie wirtualnych napędów CD/DVD/ISO.
  13. Redundantne zasilacze hotplug o sprawności minimum 94% (tzw. klasa Platinum). Minimalna moc pojedynczego zasilacza 700W.
  14. Redundantne wentylatory hotplug.
  15. Wspierane OS: Microsoft Windows Server 2019, 2016, Hyper-V Server
  16. Gwarancja i serwis świadczony przez Wykonawcę przez minimum 3 lata. Uszkodzone dyski nie podlegają zwrotowi. Wykonawca dostarczy wraz z serwerem dodatkową gwarancję producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia.

1. **Serwer typ 2 – 2 szt.**

Wymagana specyfikacja serwera.

* 1. Obudowa typu RACK 19”, maksimum 2U dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack, wraz z organizerem kabli.
  2. Płyta główna minimum dwuprocesorowa, z możliwością instalacji procesorów 28-rdzeniowych. Minimum 12 alokacji na dyski 2,5” SATA Hot – Plug. możliwość instalacji dysków SATA, SSD, SAS.
  3. Płyta główna jest obsługiwana przez wbudowany Chipset realizujący funkcję PCIe Uplink x16 (lub o wyższej krotności), umożliwiającą wykorzystanie wielu dodatkowych linii PCIe prowadzących do kontrolera płyty w celu zapewnienia wysokiej przepustowości I/O.
  4. Złącza minimum – 6 aktywnych złącz PCI Express generacji 3 w tym: 3 fizyczne złącza o prędkości x16 oraz 3 fizyczne złącza o prędkości x8.
  5. Minimum 24 gniazda z możliwością zainstalowania minimum 3TB pamięci RAM.
  6. Dwa procesory minimum 24-rdzeniowe o architekturze x86\_64, osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 160 pkt (wynik dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html. Wykonawca załączy do oferty wydruk z wyżej wymienionej strony bez jej tłumaczenia na język polski, podpisany za zgodność z oryginałem przez Wykonawcę. W przypadku braku wyników dla oferowanego procesora oferent zobowiązany jest dołączyć oświadczenie producenta serwera, w którym opierając się na wynikach dostępnych dla innego procesora tego samego typu i tego samego producenta wykaże, iż oferowany procesor spełnia wymagania minimalne.
  7. Zainstalowana pamięć RAM min. 512 GB. typu RDIMM lub LRDIMM o przepustowości min. 2666 MT/s. Pojedynczy moduł pamięci o pojemności min. 64 GB.
  8. Zainstalowane minimum: 4 dyski SAS 12G 600GB 10K 512n HOT PLUG. Dyski skonfigurowane w RAID 5.
  9. Zainstalowane minimum: 4 interfejsy LAN 1Gbit Base-T (w tym mini. 2 interfejsy ze wsparciem iSCSI oraz PXE boot), 4 interfejsy LAN 10Gbit MMF LC (z modułami SFP+ SR), interfejsy FC 2x 16Gb (z modułami SFP+ SWL).
  10. Zainstalowany kontroler RAID dla wewnętrznych dysków z 4 GB pamięci cache i podtrzymywaniem typu flash obsługujący poziomy RAID: 0,1,5,6. Kontroler RAID zainstalowany w serwerze musi obsługiwać 16 dysków (wbudowane złącza: 4x Mini-SAS HD x4) bez konieczności instalacji dodatkowych elementów (nie jest dopuszczalne stosowanie ekspanderów i dwóch kontrolerów).
  11. Zintegrowana karta graficzna ze złączem VGA, wbudowane w obudowę min. 1 port USB na panelu przednim, min. 1 port USB wewnętrzny ( lub rozwiązanie oparte na adapterze obsługującym dyski SSD M.2 w trybie RAID 1) min. 2 porty USB 3.0 dostępne z tyłu serwera..
  12. Zainstalowana i aktywna funkcja zdalnego zarządzania (konsoli) umożliwiająca: włączenie, wyłączenie, restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS), przejęcie zdalnej konsoli graficznej i podłączenie wirtualnych napędów CD/DVD/ISO.
  13. Redundantne zasilacze hotplug o sprawności minimum 94% (tzw. klasa Platinum). Minimalna moc pojedynczego zasilacza 700W.
  14. Redundantne wentylatory hotplug.
  15. Wspierane OS: Microsoft Windows Server 2019, 2016, Hyper-V Server
  16. Gwarancja i serwis świadczony przez Wykonawcę przez minimum 3 lata. Uszkodzone dyski nie podlegają zwrotowi. Wykonawca dostarczy wraz z serwerem dodatkową gwarancję producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia.

1. **Serwer typ 3 – 1 szt.**

Wymagana specyfikacja serwera.

* 1. Obudowa typu RACK 19”, maksimum 2U dostarczona wraz z szynami umożliwiającymi wysunięcie serwera z szafy rack, wraz z organizerem kabli.
  2. Płyta główna minimum dwuprocesorowa, z możliwością instalacji procesorów 28-rdzeniowych. Minimum 12 alokacji na dyski 3,5” SATA Hot – Plug. możliwość instalacji dysków SATA, SSD, SAS.
  3. Płyta główna jest obsługiwana przez wbudowany Chipset realizujący funkcję PCIe Uplink x16 (lub o wyższej krotności), umożliwiającą wykorzystanie wielu dodatkowych linii PCIe prowadzących do kontrolera płyty w celu zapewnienia wysokiej przepustowości I/O.
  4. Złącza minimum – 6 aktywnych złącz PCI Express generacji 3 w tym: 3 fizyczne złącza o prędkości x16 oraz 3 fizyczne złącza o prędkości x8.
  5. Minimum 24 gniazda z możliwością zainstalowania minimum 3TB pamięci RAM.
  6. Dwa procesory minimum 10-rdzeniowe o architekturze x86\_64, osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base minimum 119 pkt (wynik dla dwóch procesorów). Wynik musi być opublikowany na stronie https://www.spec.org/cpu2017/results/rfp2017.html. Wykonawca załączy do oferty wydruk z wyżej wymienionej strony bez jej tłumaczenia na język polski, podpisany za zgodność z oryginałem przez Wykonawcę. W przypadku braku wyników dla oferowanego procesora oferent zobowiązany jest dołączyć oświadczenie producenta serwera, w którym opierając się na wynikach dostępnych dla innego procesora tego samego typu i tego samego producenta wykaże, iż oferowany procesor spełnia wymagania minimalne.
  7. Zainstalowany RAM min. 256 GB typu RDIMM lub LRDIMM o przepustowości min. 2666 MT/s. Pojedynczy moduł pamięci o pojemności min. 64 GB.
  8. Zainstalowane minimum: 5 dysków SATA 6G 6TB 512e HOT PLUG oraz 2 dyski SAS 12G 300GB 10K 512n HOT PLUG.
  9. Zainstalowane minimum: 4 interfejsy LAN 1Gbit Base-T (w tym mini. 2 interfejsy ze wsparciem iSCSI oraz PXE boot), 4 interfejsy LAN 10Gbit MMF LC (z modułami SFP+ SR), interfejsy FC 2x 16Gb (z modułami SFP+ SWL).
  10. Zainstalowany kontroler RAID dla wewnętrznych dysków z 4 GB pamięci cache i podtrzymywaniem typu flash obsługujący poziomy RAID: 0,1,5,6. Kontroler RAID zainstalowany w serwerze musi obsługiwać 16 dysków (wbudowane złącza: 4x Mini-SAS HD x4) bez konieczności instalacji dodatkowych elementów (nie jest dopuszczalne stosowanie ekspanderów i dwóch kontrolerów).
  11. Zintegrowana karta graficzna ze złączem VGA, wbudowane w obudowę min. 1 port USB na panelu przednim, min. 1 port USB wewnętrzny ( lub rozwiązanie oparte na adapterze obsługującym dyski SSD M.2 w trybie RAID 1) min. 2 porty USB 3.0 dostępne z tyłu serwera.
  12. Zainstalowana i aktywna funkcja zdalnego zarządzania (konsoli) umożliwiająca: włączenie, wyłączenie, restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS), przejęcie zdalnej konsoli graficznej i podłączenie wirtualnych napędów CD/DVD/ISO.
  13. Redundantne zasilacze hotplug o sprawności minimum 94% (tzw. klasa Platinum). Minimalna moc pojedynczego zasilacza 700W
  14. Redundantne wentylatory hotplug.
  15. Wspierane OS: Microsoft Windows Server 2019, 2016, Hyper-V Server
  16. Gwarancja i serwis świadczony przez Wykonawcę przez minimum 3 lata. Uszkodzone dyski nie podlegają zwrotowi. Wykonawca dostarczy wraz z serwerem dodatkową gwarancję producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia.

1. **Oprogramowanie – system operacyjny serwerów typ 1 i 2 w ilości 4 szt.**
   1. Wykonawca dostarczy 4 szt. licencji na system operacyjny Microsoft Windows Server 2019 Datacenter wraz z licencjami na środowisko wirtualne Hyper-v (bez limitu maszyn wirtualnych) licencjonowany na dostarczane serwery typu 1 i 2 (dopuszczalne oprogramowanie nowsze z możliwością zainstalowania niższej wersji) lub system operacyjny - oprogramowanie równoważne. Dopuszczalne licencje zbiorcze lub powiązane ze sprzętem.
   2. Oprogramowanie równoważne musi spełniać następujące minimalne wymagania.
   3. Obsługa funkcji systemu operacyjnego serwera dla serwerów typ 1 i 2.
   4. Obsługa zarządzania i instalacji nielimitowanej ilości maszyn wirtualnych w środowisku Hyper-v.
   5. Natywnie wbudowana możliwość integracji z posiadanymi przez Zamawiającego systemami Windows Server i systemem domenowym Active Directory,
   6. Zawarta licencja na uruchamianie na serwerze fizycznym w środowisku wirtualnym nieograniczonej licencyjnie liczby wirtualnych instancji systemów Windows oraz oprogramowania zakupionego przez Zamawiającego działającego na systemach serwerowych MS Windows.
   7. Możliwość tworzenia serwerów wirtualnych i łączenia ich w klastry z systemami wirtualnymi MS Hyper-V.
   8. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na tworzenie maszyn wirtualnych.
   9. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności muszą mieć możliwość przenoszenia pomiędzy serwerami klastra typu failover.
   10. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
   11. System operacyjny musi posiadać graficzny interfejs użytkownika.
   12. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

a. zarządzania użytkownikami,

b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,

c. możliwość przydzielania praw dostępu do zasobów sieciowych,

d. instalacji zdalnej oprogramowania z pakietów msi,

e. definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows:7, 10.

* 1. Oprogramowanie powinno umożliwiać uruchomienie serwera usług terminalowych oraz zdalnego pulpitu RDP.

1. **Oprogramowanie – system operacyjny serwera typ 3, w ilości 1 szt.**
   1. Licencje na system operacyjny Microsoft Windows Server 2019 Standard licencjonowany na dostarczany serwer typu 3 (dopuszczalne oprogramowanie nowsze z możliwością zainstalowania niższej wersji) lub system operacyjny - oprogramowanie równoważne. Dopuszczalne licencje zbiorcze lub powiązane ze sprzętem.
   2. Oprogramowanie równoważne musi spełniać następujące minimalne wymagania.
   3. Obsługa funkcji systemu operacyjnego serwera dla serwerów typ 3.
   4. Natywnie wbudowana możliwość integracji z posiadanymi przez Zamawiającego systemami Windows Server i systemem domenowym Active Directory,
   5. Zawarta licencja na uruchamianie na serwerze fizycznym w środowisku wirtualnym wirtualnych minimum 2 instancji systemu operacyjnego Windows oraz oprogramowania zakupionego przez Zamawiającego działającego na systemach serwerowych MS Windows.
   6. Możliwość tworzenia serwerów wirtualnych i łączenia ich w klastry z systemami wirtualnymi MS Hyper-V.
   7. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na tworzenie maszyn wirtualnych.
   8. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności muszą mieć możliwość przenoszenia pomiędzy serwerami klastra typu failover.
   9. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
   10. System operacyjny musi posiadać graficzny interfejs użytkownika.
   11. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:

a. zarządzania użytkownikami,

b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,

c. możliwość przydzielania praw dostępu do zasobów sieciowych,

d. instalacji zdalnej oprogramowania z pakietów msi,

e. definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows:7, 10.

* 1. Oprogramowanie powinno umożliwiać uruchomienie serwera usług terminalowych oraz zdalnego pulpitu RDP.

1. **Dodatkowe oprogramowanie**
   1. Wykonawca dostarczy pakiet licencji dostępowych do w/w serwerowych systemów operacyjnych dla użytkowników wewnętrznych w ilości 100 szt. oraz użytkowników terminalowych w technologii RDP w ilości 100 szt. Licencje muszą zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników wewnętrznych funkcjonalności serwerowych systemów operacyjnych.
2. **Zasilacz UPS do podtrzymywania środowiska serwerowego** **do montażu w szafie typu RACK 19” w ilości 2 szt.**
   1. Obudowa z możliwością instalacji w standardowej szafie serwerowej rack 19” z zajętością nie więcej niż 4U. Urządzenie będzie dostarczone wraz z niezbędnymi akcesoriami do montażu w szafie RACK.
   2. Moc pozorna nie mniej niż 3000 VA, moc skuteczna nie mniej niż 2700 W.
   3. Gniazdo wejściowe typu IEC320 C20 (minimum 16A), minimum 7 gniazd wyjściowych typu IEC320-C13 (10A), minimum 1 gniazdo wyjściowe typu IEC320-C19 (16A)
   4. Częstotliwość 50/60 Hz (+/-3) Hz
   5. Zasilacz dostarczony z bateriami umożliwiającymi na podtrzymania zasilania dla obciążenia 50%: nie mniej niż 20 min oraz czas podtrzymania dla obciążenia 100%: nie mniej niż 10 min. Napięcie wejściowe - co najmniej w zakresie: 160 - 275V
   6. Czas przełączania nie więcej niż 10 ms.
   7. Kształt napięcia wyjściowego: sinusoidalny.
   8. Możliwość zwiększenia czasu podtrzymania zasilania przez rozszerzenie o dodatkowe moduły bateryjne.
   9. Porty komunikacyjne USB, RJ-45 10/100 Base-T , serial, zamontowana karta sieciowa pozwalająca na zdalne zarządzanie urządzeniem za pośrednictwem przeglądarki WWW i ssh.
   10. Wyposażenie standardowe: instrukcja obsługi w języku polskim lub angielskim, oprogramowanie, kabel USB, kabel szeregowy, kable zasilające.
   11. Automatyczna regulacja napięcia (AVR)
   12. Zabezpieczenie przeciwprzepięciowe
   13. Wczesne ostrzeganie o stanie zasilacza UPS
   14. Pełne sekwencyjne testowanie akumulatorów
   15. Zdalne awaryjne wyłączanie zasilania
   16. Możliwość wymiany akumulatorów przez użytkownika w czasie pracy urządzenia
   17. Gwarancja i serwis świadczony przez Wykonawcę przez min. 3 lata na elektronikę i 2 lata na baterię akumulatorów. Udzielona gwarancja nie może ograniczać rozbudowy lub rekonfiguracji o ile będą one wykonywane zgodnie z wymogami technicznymi producenta.
3. **Szafa serwerowa** **typu RACK 19” 42U w ilości 1szt.**
   1. Wysokość wewnętrzna 42U.
   2. Nośność nie mniej niż 1000 kg.
   3. Kolor czarny lub grafit.
   4. Perforowane drzwi przednie wykonane z blachy:
   5. Dodatkowe informacje dot. drzwi przednich:

- otwierane do 180 stopni;

- możliwość montażu lewo/prawo;

- zamek z kluczem.

* 1. Perforowane drzwi tylne, wykonane z blachy.
  2. Dodatkowe informacje dot. drzwi tylnych - 2 skrzydła otwierane:

- zamek z kluczem;

- zdejmowane ścianki boczne.

* 1. Sufit wyposażony w otwory dla paneli wentylacyjnych:

- dodatkowe stopy zapewniające stabilność szafy;

- uziemienie;

- otwory do pasywnych i aktywnych wentylacji.

* 1. Gwarancja i serwis świadczony przez Wykonawcę przez min. 3 lata. Wymiana lub naprawa w miejscu eksploatacji.

1. Wdrożenie: Zamawiający dostarczy sprzęt i oprogramowanie do siedziby Zamawiającego oraz zamontuje i zainstaluje sprzęt, oprogramowanie systemowe i wirtualizacyjne. Wykonawca podłączy urządzenia do sieci Zamawiającego oraz zainstaluje najnowsze oprogramowanie firmware i aktualizacje systemowe.
2. Wykonawca przeprowadzi instruktaż trwający przynajmniej 4 godziny dla minimum 3 administratorów Zamawiającego. Szkolenie będzie przeprowadzone w siedzibie Zamawiającego.
   * 1. **Część II**

Dostarczone w ramach części II poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:

* 1. Wszystkie oferowane urządzenia muszą być fabrycznie nowe (na dzień dostawy urządzenia nie mogą być starsze niż 6 miesięcy od daty produkcji oraz nie mogą być używane).
  2. Oferowany sprzęt musi pochodzić z produkcji seryjnej.
  3. Dla dostarczanych rozwiązań musi istnieć możliwość wykupienia wsparcia technicznego u producenta danego rozwiązania.
  4. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO9001:2000 lub normą równoważną. Zgodne z prawem obowiązującym w Unii Europejskiej dostarczone elementy infrastruktury muszą spełniać wytyczne dyrektywy CE (Conformité Européenne) i muszą być oznaczone znakiem CE.
  5. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
  6. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
  7. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: wkładek optycznych, kabli zasilających, kabli FC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
  8. Na dzień złożenia oferty oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
  9. Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca  zobowiązany  jest  do udzielenia  niewyłącznej  licencji(na oprogramowanie) Zamawiającemu  lub  przeniesie  na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.

1. **Macierz dyskowa – 2 szt.**

Wymagana specyfikacja macierzy.

* 1. Macierz musi być dostarczona ze wszystkimi elementami do instalacji w szafie rack 19''
  2. Macierz musi zostać dostarczona w konfiguracji zawierającej minimum: 21 dyski 3,8 TB SAS SSD. Macierz musi mieć minimum 24 zatoki na dyski 2.5 calowe. Macierz musi wspierać dyski 2,5” i 3,5”. Macierz musi mieć możliwość zainstalowania minimum 144 dysków (zarówno SSD jak i SAS) wyłącznie poprzez dodanie półek dyskowych.
  3. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”,a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania - odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu/firmware’u macierzy w trybie online bez wyłączania interfejsów macierzy.
  4. Macierz musi posiadać minimum 2 kontrolery pracujące redundantnie Active – Active, umożliwiające rozbudowę do pracy w układzie klastra. Praca w układzie klastra musi zapewniać dostęp do danych składowanych na dowolnych półkach obu macierzy poprzez każdy z dwóch kontrolerów dostarczanych macierzy przez porty FC i Ethernet dla wszystkich wymaganych poniżej protokołów. Każdy kontroler musi posiadać identyczną konfigurację, tzn. liczbę i parametry CPU, parametry i pojemność pamięci cache, parametry i liczbę portów we/wy. Komunikacja pomiędzy wszystkimi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę, nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband).
  5. W przypadku klastrowania kontrolerów macierzy, system musi działać pod kontrolą jednego systemu operacyjnego od jednego producenta, nie dopuszczalne jest zestawienie systemu klastrowego poprzez wykorzystanie serwerów pośredniczących i oprogramowania dodatkowego. Musi być możliwość rozbudowy rozwiązania do co najmniej 6 kontrolerów w klastrze dla rozwiązania SAN i 8 kontrolerów dla rozwiązania NAS – połączenie w klastrze za pomocą interfejsów minimum 10 GbE SFP+.
  6. Macierz wyposażona w przynajmniej 64GB pamięci RAM (32 GB na kontroler) w tym minimum 8GB pamięci NVRAM (4 GB na kontroler). W przypadku awarii zasilania dane niezapisane na dyskach, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez czas niezbędny do zapisana na dysku.
  7. Dwa kontrolery wyposażone w minimum 1 TB pamięci NVME flash cache (na każdy kontroler) dedykowanej do odczytu.
  8. Macierz musi posiadać minimum 4 porty FC 16 Gbps (z modułami multi-mode), 4 porty 10GbE SFP+ (z modułami multi-mode). Wszystkie porty muszą zapewniać wykorzystanie do transmisji danych w relacji do serwerów.
  9. Macierz musi pozwalać na równoczesne zabezpieczenie dysków w grupach RAID0, RAID1, RAID5, RAID6, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy lub rozwiązanie oparte na zabezpieczeniu dysków w grupach RAID-4, RAID-DP, RAID-TEC, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy.
  10. Kopie migawkowe - Macierz musi być wyposażona w jednolity system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy (plikowych i blokowych).
  11. Obsługiwane protokoły - Macierz musi obsługiwać protokół FC, iSCSI, CIFS i NFS - jeśli wymagana jest licencja zamawiający wymaga dostarczenia jej wraz z macierzą.
  12. Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych dla dysków SSD i SAS.
  13. Macierz musi posiadać funkcjonalność kompresji danych na dyskach SSD i SAS.
  14. Macierz musi posiadać funkcjonalność kompresji danych w trybie in-line oraz postprocess dla każdego obsługiwanego rodzaju danych.
  15. Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych, którą można stosować na macierzy/danych produkcyjnych dla wszystkich rodzajów danych. Macierz musi mieć możliwość wykonania czynności odwrotnej, tzn. cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie.
  16. Macierz musi posiadać możliwość replikacji danych z inna macierzą tego samego producenta w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy.
  17. Macierz musi posiadać funkcjonalność klonowania danych bez potrzeby fizycznego kopiowania danych na nośnikach.
  18. Macierz musi posiadać funkcjonalność pozwalającą na odzyskiwanie danych ze snapshotów bez potrzeby kopiowania danych.
  19. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows 2016/2019, Linux, VMware.
  20. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie
  21. Macierz musi pozwalać na integrację z VMware, MS HyperV.
  22. Macierz musi posiadać funkcjonalność priorytetyzacji zadań.
  23. Macierz musi posiadać możliwość automatycznego informowania przez macierz o zdarzeniach i przesyłania ich przez pocztę elektroniczną.
  24. Wszystkie funkcjonalności muszą być dostarczone licencyjnie na maksymalną możliwą do uzyskania po ewentualnej rozbudowie pojemność macierzy.
  25. Zarządzanie macierzą musi być realizowane graficznie za pośrednictwem przeglądarki WWW umożliwiającą sprawdzanie poprawności działania macierzy.
  26. Gwarancja i serwis świadczony przez Wykonawcę przez minimum 3 lata, 3 lata subskrypcji oprogramowania, w przypadku awarii dyski uszkodzone pozostają u Zamawiającego.
  27. Jeżeli jakakolwiek z funkcjonalności dostarczonego rozwiązania będzie wymagała dodatkowej licencji należy ją dostarczyć wraz z urządzeniem. Elementy, z których zbudowana jest macierz muszą być produktami producenta tej macierzy lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne.
  28. Wykonawca dostarczy dokumentację techniczną w języku polskim lub angielskim.

1. Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum: instalację fizyczną, podłączenie do sieci LAN/SAN, podłączenie do istniejącej sieci Zamawiającego, aktualizację oprogramowania systemowego urządzenia, instalację jednej puli dyskowej i jej prezentacja do min. 2 serwerów.
2. Wykonawca przeprowadzi instruktaż trwający przynajmniej 4 godziny dla 3 administratorów Zamawiającego. Szkolenie będzie przeprowadzone w siedzibie Zamawiającego.

**III. Część III**

1. Dostarczone w ramach części III poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:
   1. Wszystkie oferowane urządzenia muszą być fabrycznie nowe (na dzień dostawy urządzenia nie mogą być starsze niż 6 miesięcy od daty produkcji oraz nie mogą być używane).
   2. Oferowany sprzęt musi pochodzić z produkcji seryjnej.
   3. Dla dostarczanych rozwiązań musi istnieć możliwość wykupienia wsparcia technicznego u producenta danego rozwiązania.
   4. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO9001:2000 lub normą równoważną. Zgodne z prawem obowiązującym w Unii Europejskiej dostarczone elementy infrastruktury muszą spełniać wytyczne dyrektywy CE (Conformité Européenne) i muszą być oznaczone znakiem CE.
   5. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
   6. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
   7. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: wkładek optycznych, kabli zasilających, kabli FC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
   8. Na dzień złożenia oferty oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
   9. Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji(na programowanie) Zamawiającemu lub przeniesie na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.
2. **Przełącznik FibreChannel – 2 szt.**

Wymagana specyfikacja przełącznika.

* 1. Wysokość przełącznika maksimum 1U z systemem montażu w szafie typu rack 19”.
  2. Możliwość zainstalowania portów SFP minimum: 24 szt. porty uniwersalne o maksymalnej przepustowości 16GB/s, z obsługą przepustowości 8Gbit/s i 4Gbit/s z automatycznym wyborem przepustowości (auto-sensing), obsługa trybu full-duplex.
  3. Zainstalowane 16 aktywnych portów z modułami optycznymi SFP+ 16Gbit/s, Short Wave Length (SWL). Obsługa trybów pracy portów FC: D\_port, F\_port, E\_port, M-Port.
  4. Przełącznik dostarczony z 16 wkładkami SFP+, krótkodystansowych, ze złączem LC o prędkości 16 Gbit każda z możliwością wymiany bez konieczności wyłączenia oraz kompletem kabli i przewodów.
  5. Możliwość aktualizacji firmware’u przełącznika w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
  6. Aktywne funkcje: zarządzanie graficzne, zaawansowany Zoning, pełny Fabric, ISL Trunking.
  7. Możliwość rozbudowy o obsługę funkcjonalności (przez zakupienie odpowiednich licencji).
  8. Zarządzanie: port RJ-45 minimum 10/100 Mb/s do zarządzania poprzez sieć Ethernet, port RJ-45 do zarządzania poprzez interfejs RS232.
  9. Sygnalizacja aktywnych i podłączonych portów na panelu przednim urządzenia.
  10. Zarządzanie poprzez przeglądarkę WWW z obsługą połączeń szyfrowanych SSL oraz poprzez usługę SSH.
  11. Urządzenia dostarczone będą wraz z:

a. Wymaganymi kablami konsolowymi i zasilającymi 240V.

b. 24 szt patchcord LC/LC, o długości 3m

* 1. Dostarczone rozwiązanie musi posiadać min. 3 lata gwarancji z naprawą w miejscu instalacji urządzenia i z gwarantowanym czasem skutecznego zakończenia naprawy najpóźniej w ciągu następnego dnia roboczego od dnia zgłoszenia awarii do serwisu producenta.

1. **Przełącznik Ethernet – 2 szt.**

Wymagana specyfikacja przełącznika.

* 1. Obudowa (chassis) modularna z wyposażeniem do montażu w szafie 19” Rack, posiadająca min. 6 slotów (złącz) na moduły liniowe oraz zasilacze w ilości i konfiguracji niezbędnej do zapewnienia redundancji zasilania, 240 VAC, 50/ 60 Hz.
  2. Możliwość zainstalowania minimum 144 portów 10/100/1000 Base-T, lub 48 portów typu SFP+ lub 12 portów 40 GbE (z możliwością kombinacji).
  3. Zainstalowane porty minimum: 16 portów 10GbE SFP+ z modułami optycznymi 10G SFP+ LC SR, 40 portów 1 GbE BASE-T RJ45.
  4. Zainstalowane minimum 2 redundantne moduły zarządzające.
  5. Przepustowość minimum 570 Mpps.
  6. Wydajność routowania / przełączania min. 960 Gbps.
  7. Prędkość matrycy przełączającej min. 1015 Gbps.
  8. Pojemność tabeli adresów MAC min. 64000.
  9. Obsługa standardów: IEEE 802.1ad Q-in-Q, IEEE 802.1AX-2008 Link Aggregation, IEEE 802.1D MAC Bridges, IEEE 802.1p Priority, IEEE 802.1Q VLANs, IEEE 802.1s Multiple Spanning Trees, IEEE 802.1v VLAN classification by Protocol and Port, IEEE 802.1w Rapid Reconfiguration of Spanning Tree, IEEE 802.3ad Link Aggregation Control Protocol (LACP), IEEE 802.3af Power over Ethernet, IEEE 802.3az Energy Efficient Ethernet, IEEE 802.3x Flow Control, IEEE 802.3bz 2.5Gb/s and 5Gb/s interfaces, RFC 768 UDP, RFC 783 TFTP Protocol (revision 2), RFC 792 ICMP, RFC 793 TCP, RFC 826 ARP, RFC 854 TELNET, RFC 868 Time Protocol, RFC 951 BOOTP, RFC 1058 RIPv1, RFC 1350 TFTP Protocol (revision 2), RFC 1519 CIDR, RFC 1542 BOOTP Extensions, RFC 1918 Address Allocation for Private Internet, RFC 2030 Simple Network Time Protocol (SNTP) v4, RFC 2131 DHCP, RFC 2453 RIPv2, RFC 2548 (MS-RAS-Vendor only), RFC 3046 DHCP Relay Agent Information Option, RFC 3575 IANA Considerations for RADIUS, RFC 3576 Ext to RADIUS (CoA only), RFC 3768 VRRP, RFC 4675 RADIUS VLAN & Priority, RFC 5880 Bidirectional Forwarding Detection, RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification, UDLD (Uni-directional Link Detection).
  10. Dostarczone rozwiązanie musi posiadać min. 3 lata gwarancji z naprawą w miejscu instalacji urządzenia i z gwarantowanym czasem skutecznego zakończenia naprawy najpóźniej w ciągu następnego dnia roboczego od dnia zgłoszenia awarii do serwisu producenta.

1. Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum: instalację fizyczną, podłączenie do sieci LAN/SAN, podłączenie do istniejącej sieci Zamawiającego, aktualizację oprogramowania systemowego urządzenia.
2. Wykonawca przeprowadzi instruktaż trwający przynajmniej 4 godziny dla minimum 3 administratorów Zamawiającego. Szkolenie będzie przeprowadzone w siedzibie Zamawiającego.
   * 1. **Część IV**
   1. Dla dostarczanych rozwiązań dostarczanych w ramach części IV musi istnieć możliwość wykupienia wsparcia technicznego u producenta danego rozwiązania.
   2. Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca  zobowiązany  jest  do udzielenia  niewyłącznej  licencji(na oprogramowanie) Zamawiającemu  lub  przeniesie  na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.
3. **Oprogramowanie do backupu i HA dla dostarczanych serwerów 1,2 i 3.**

Wymagana specyfikacja oprogramowania do backupu i HA (High Availability).

* 1. Dostarczone oprogramowanie musi spełniać wszystkie poniższe wymagania.
     1. Oprogramowanie musi umożliwiać zarządzanie wszystkimi własnymi funkcjami z centralnego serwera - oraz korzystać z polityk i reguł wykonywania operacji zabezpieczania i odtwarzania danych, zbudowanych przez Zamawiającego.
     2. Oprogramowanie musi zapewniać zapis kopii zapasowych w formacie szyfrowanym z uwzględnieniem deduplikacji globalnej wszystkich kopii zapasowych ze wszystkich dostarczanych komputerów na serwerze centralnym systemu.
     3. Oprogramowanie w formie licencji musi zapewniać dla systemów działających pod kontrolą systemu Windows:  
        - pełne zarządzanie wszystkimi swoimi funkcjami za pomocą oprogramowania serwera centralnego zarządzania,

- korzystanie z polityk stworzonych przez Zamawiającego na serwerze centralnego zarządzania,

- wykonywanie pełnej replikacji maszyny fizycznej do wirtualnej (P2V) i wirtualnej do wirtualnej (V2V) w środowiskach Microsoft Hyper-V, VMware vSphere lub Citrix XenServer, umożliwiającej automatyczne lub ręczne uruchomienie maszyny zapasowej,

- przywracanie stanu z kopii zapasowej do dowolnego punktu w czasie (w ramach zadeklarowanego okresu czasu),

- możliwość wykonania pełnych testów stanu repliki (pod względem sprawności działania środowiska produkcyjnego bez konieczności przerywania replikacji),

- możliwość granularnego odczytu danych zapisanych w kopiach zapasowych.

* + 1. Oprogramowanie musi być licencjonowane na procesory fizyczne w liczbie wynikającej z liczby procesorów zainstalowanych w dostarczanych w zadaniu 1 serwerach. Oprogramowanie w zakresie funkcji wysokiej dostępności (High Availability) może być licencjonowane „per Host” tzn. na pojedynczy hypervisor w ilości zgodnej z liczbą maszyn fizyczych (5 szt.).
    2. Funkcje oprogramowania licencjonowane na procesory fizyczne muszą zapewniać uruchomienie wszystkich przypisanych im funkcjonalności, dla serwerów fizycznych, nielimitowanej liczby serwerów wirtualnych, nielimitowanej liczby baz i aplikacji oraz nielimitowanej ilości danych.
    3. Funkcje oprogramowania licencjonowane „per Host” muszą zapewniać uruchomienie wszystkich przypisanych im funkcjonalności, dla 5 hypervisor’ów, z nielimitowaną liczbą serwerów wirtualnych oraz nielimitowanej ilości danych.
    4. Oprogramowanie musi posiadać, opisane w dokumentacji produktu, wsparcie producenta oprogramowania na instalację systemu zarządzania nim na platformie wirtualnej.
    5. O Oprogramowanie musi zapewniać utworzenie repozytorium backupu, tj. wykonywanie backupu bezpośrednio na dyskach lokalnych, dyskach przenośnych, macierzach dyskowych SAN i NAS, jak również w chmurze (Microsoft Windows Azure, Amazon Web Services), zapewniając równocześnie:

- możliwość replikacji tego repozytorium backupu do innej lokalizacji / innego repozytorium,

- możliwość zainicjalizowania wyżej wymienionej replikacji w trybie offline (np. za pomocą nośnika przenośnego) tj. bez konieczności przesyłania przez sieć na nośnik docelowy, całej zawartości źródłowego repozytorium backupu.

- możliwość utworzenia wielu repozytoriów backupu jednocześnie na różnych wymienionych powyżej nośnikach,

- optymalizację replikacji dla łącz WAN

* + 1. Oprogramowanie musi wykonywać backup bezpośrednio do repozytorium oparty o technologię przyrostowej kopii migawkowej na poziomie bloków danych, to znaczy – tylko pierwszy backup jest pełny, pozostałe wieczyście tylko przyrostowe (bez konieczności wykonywania ponownie kopii pełnych), dla serwerów fizycznych i wirtualnych – zapewniający równocześnie:

- spójny backup do repozytorium, bez konieczności zatrzymywania, aplikacji MS Exchange, MS SQL i Oracle, umożliwiający odtworzenie ich jako spójnej i działającej aplikacji,

- możliwość odtworzenia pojedynczego maila z serwera Exchange,

- możliwość odtworzenia pojedynczego pliku i folderu systemu plikowego,

- możliwość odtworzenia backupu bezpośrednio z repozytorium w oparciu o mechanizm Bare Metal Recovery polegający na odtworzeniu całych serwerów fizycznych i wirtualnych w jednym procesie, bezpośrednio z repozytorium backupowego, bez wcześniejszego instalowania na nich jakichkolwiek systemów operacyjnych, sterowników, agentów backupu, itd. dla systemów Windows i Linux

- możliwość odtworzenia całego serwera fizycznego w oparciu o mechanizm Bare Metal Recovery na dowolną maszynę fizyczną lub wirtualną dla systemów Windows i Linux

- możliwość odtworzenia całego serwera wirtualnego w oparciu o mechanizm Bare Metal Recovery na dowolną maszynę fizyczna lub wirtualną dla systemów Windows i Linux

- możliwość odtworzenia serwera pełniącego funkcję kontrolera domeny Active Directory

- możliwość automatycznego uruchamiania przez oprogramowanie backupowe poleceń na serwerze backupowanym przed i po wykonaniu backupu

- backup serwerów wirtualnych na poziomie Hypervisora bez konieczności instalacji oprogramowania na systemie Gościa (Guest)

- możliwość backupu maszyn wirtualnych z poziomu Hypervisora, niezależnie od tego czy maszyna wirtualna jest włączona – świadczy usługi, wstrzymana, czy też całkowicie wyłączona, za pomocą tego samego zadania backupu, bez konieczności jego modyfikowania,

- możliwość wykonywania, wyłącznie za pomocą oprogramowania backupowego (bez pomocy zewnętrznych skryptów i z wykorzystaniem wyłącznie MS Hyper-V i VMware), kopii zapasowej tak, aby posiadała wszystkie cechy maszyny wirtualnej, zapewniające możliwość automatycznego i ręcznego uruchomienia kopii zapasowej, za pomocą tego samego oprogramowania backupowego, od razu jako działającej maszyny wirtualnej na platformie MS Hyper-V lub VMware, bez konieczności korzystania z mechanizmów odtwarzania samego backupu,

- możliwość odtworzenia systemów fizycznych i wirtualnych przy użyciu Bare Metal Recovery z backupu w przypadkach odtworzenia systemu z backupu na maszynie zgodnej z BIOS z backupu wykonanego na maszynie zgodnej z uEFI oraz w przypadkach odtworzenia systemu z backupu na maszynie zgodnej z uEFI z backupu wykonanego na maszynie zgodnej z BIOS,

- szyfrowanie danych backupu (min. AES-256),

- kompresję danych backupu,

- globalną deduplikację danych na poziomie klienta (przed przesłaniem do repozytorium backupu – przez sieć przesyłane są tylko unikalne bloki danych) dla wszystkich danych, ze wszystkich źródeł, znajdujących się w repozytorium,

- możliwość eksportu z repozytorium dowolnego backupu, wyniku pojedynczego zadania backupowego, na nośnik zewnętrzny,

- możliwość ograniczenia pasma sieciowego używanego przez system backupu według harmonogramu,

- możliwość ręcznego i automatycznego backupu danych z repozytorium dyskowego na taśmę,

* + 1. Oprogramowanie musi umożliwiać wykonanie konwersji systemu na inną platformę sprzętową w trybie, niezależnie od tego, czy maszyna pracuje pod kontrolą BIOS czy uEFI (konwersja BIOS->uEFI, konwersja uEFI→BIOS): system fizyczny do innego systemu fizycznego (inna platforma sprzętowa), system fizyczny do systemu wirtualnego, system wirtualny do systemu fizycznego, system wirtualny do innego systemu wirtualnego, lub może wykorzystywać narzędzia konwersyjne dostarczane przez producentów systemów operacyjnych.
    2. Oprogramowanie musi zapewniać możliwość pełnego centralnego zarządzania przez www modułem wykonywania kopii migawkowych na serwerach źródłowych w zakresie:

- importu systemów do backupu z systemu Microsoft Active Directory

- instalacji oprogramowania do wykonywania kopii migawkowych

- konfiguracji parametrów wykonywania kopii migawkowych

- przydzielania zadań wykonywania kopii migawkowych

- monitorowania stanu wykonania kopii migawkowych

- powiadamiania o stanie zadań backupu drogą mailową

- przeglądania i odtwarzania wybranych elementów wykonanych kopii migawkowych

- monitorowania w trybie graficznym aktualnego stanu systemu z uwzględnieniem: statusu wykonanych zadań backupu (udane/nieudane), aktualnej wielkości danych backupowych, aktualnej zajętości repozytorium backupu, trendów objętości backupu, wielkości danych w repozytoriach backupu z uwzględnieniem rzeczywistej, wielkości danych źródłowych i objętości z uwzględnieniem kompresji i deduplikacji, dostępu do w/w informacji, z głównego ekranu konsoli do zarządzania oprogramowaniem, za pomocą nie więcej niż dwóch kliknięć myszy.

* + 1. Oprogramowanie musi zapewniać wsparcie dla systemów operacyjnych systemów fizycznych: Windows 2016, Windows 2019, Windows 10
    2. Oprogramowanie musi zapewniać wsparcie dla baz danych: MS SQL Server oraz Oracle,
    3. Oprogramowanie musi zapewniać wsparcie dla systemów wirtualizacyjnych: Microsoft Hyper-v Server 2016, Microsoft Hyper-v Server 2019
    4. Oprogramowanie musi zapewniać możliwość backupu danych (wybrane pliki, całe systemy, serwery wirtualne, aplikacje) bezpośrednio na taśmę, oraz możliwość backupu danych (wybrane pliki, całe systemy, serwery wirtualne, aplikacje) na zasób dyskowy a następnie ręcznie i automatycznie na taśmę.
    5. Oprogramowanie musi zapewniać możliwość wykonywania backupu na współdzieloną bibliotekę taśmową poprzez sieć SAN oraz możliwość backupu zasobów macierzy dyskowych przy użyciu protokołu NDMP.
    6. Oprogramowanie musi zapewniać możliwość replikacji plików i folderów pomiędzy serwerami MS Windows, niezależnie czy są to serwery fizyczne czy wirtualne, zapewniającej:

- stałe monitorowanie procesu replikacji z konsoli zarządzającej, obejmujące stan procesu i jego parametry: ilość danych oczekujących na przesłanie, ilość utworzonych/zmienionych/usuniętych folderów na systemie źródłowym, Ilość danych przesłanych, szybkość przesyłania,

- automatyczne generowanie raportów o stanie replikacji,

- automatyczne i ręczne uruchomianie kontynuacji replikacji po restarcie lub zatrzymaniu procesu, bez konieczności replikacji wszystkich danych,

- powiadamianie o zdarzeniach za pomocą maila oraz automatycznie uruchamianego skryptu,

- integralność replikowanych plików

- optymalizację replikacji dla łącz WAN

- możliwość uruchomienia replikacji na poziomie plików i bloków danych

- możliwość ustawienia częstotliwości replikacji: w trybie ciągłym – automatyczna replikacja danych plików lub bloków (w zależności od wybranego rodzaju replikacji) pomiędzy zasobem źródłowym a docelowym w chwili zakończenia modyfikacji pliku lub bloku danych, na żądanie, co określony przedział czasu, według kalendarza (z uwzględnieniem godzin, dni tygodnia i konkretnych dat)

* + 1. Oprogramowanie musi zapewniać możliwość uruchomienia replikacji w trybie wiele do jednego, tzn. dane z wielu serwerów Windows są replikowane do jednego serwera.
    2. Wsparcie techniczne producenta – minimum 3 lata (w zakresie pomocy przy zgłaszaniu problemów technicznych i prawem pobierania poprawek i nowych wersji oprogramowania oraz dostęp do bazy wiedzy).
    3. Oprogramowanie nie może w żaden sposób generować konfliktów w zakresie ruchu sieciowego jak i procesów backupowych realizowanych w infrastrukturze zamawiającego Niedopuszczalne jest spowodowanie utraty danych, czy przerw w pracy w wyniku instalacji lub wdrożenia dostarczanego oprogramowania.

1. **Oprogramowanie do backupu stacji roboczych – 100 licencji**

Wymagana specyfikacja oprogramowania do backupu stacji roboczych. Dopuszczalne licencje zbiorcze.

* 1. Oprogramowanie musi umożliwiać backup oprogramowania i danych jednocześnie ze 100 komputerów fizycznych na centralnym systemie backupu.
  2. Oprogramowanie musi obsługiwać komputery z zainstalowanym systemem operacyjnym Windows 7, Windows 10 i Linux;
  3. Oprogramowanie musi zapewniać zapis kopii zapasowych w formacie szyfrowanym z uwzględnieniem deduplikacji globalnej.
  4. Wsparcie techniczne producenta – minimum 3 lata (w zakresie pomocy przy zgłaszaniu problemów technicznych i prawem pobierania poprawek i nowych wersji oprogramowania).

1. Wykonawca przeprowadzi instruktarz stanowiskowy dla 3 pracowników Zamawiającego w zakresie obsługi administracyjnej dostarczonych rozwiązań.
2. Wykonawca zrealizuje sesję trwającą 3 dni. W sesji będzie brało udział 3 pracowników Zamawiającego.
3. Sesja instruktarzowa będzie prowadzona w miejscu wskazanym przez Wykonawcę.
4. Wszystkie koszty instruktarzu stanowiskowego pokrywa wykonawca. Dla sesji odbywającej się poza miejscem instalacji systemów Wykonawca pokrywa koszt wyżywienia oraz noclegów.
   * 1. **Część V**
5. Dostarczone w ramach części V poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:
   1. Wszystkie oferowane urządzenia muszą być fabrycznie nowe (na dzień dostawy urządzenia nie mogą być starsze niż 6 miesięcy od daty produkcji oraz nie mogą być używane).
   2. Oferowany sprzęt musi pochodzić z produkcji seryjnej.
   3. Dla dostarczanych rozwiązań musi istnieć możliwość wykupienia wsparcia technicznego u producenta danego rozwiązania.
   4. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO9001:2000 lub normą równoważną. Zgodne z prawem obowiązującym w Unii Europejskiej dostarczone elementy infrastruktury muszą spełniać wytyczne dyrektywy CE (Conformité Européenne) i muszą być oznaczone znakiem CE.
   5. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
   6. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
   7. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: wkładek optycznych, kabli zasilających, kabli FC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
   8. Na dzień złożenia oferty oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
   9. Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca  zobowiązany  jest  do udzielenia  niewyłącznej  licencji(na oprogramowanie) Zamawiającemu  lub  przeniesie  na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.
6. **Sieciowe urządzenia typu Firewall do ochrony brzegowej sieci komputerowych LAN 1 kpl.**
   1. Zapora sieciowa (firewall) musi być dostarczona w postaci dwóch dedykowanych urządzeń sieciowych (Appliance) umożliwiających pracę zarówno w konfiguracji Active-Passive, jak również Active-Active. Dedykowane urządzenia sieciowe muszą posiadać zainstalowane oprogramowanie, pochodzące od tego samego producenta.
   2. System zabezpieczeń funkcji firewall umożliwia ochronę sieci bez ograniczeń dla liczby adresów IP.
   3. Zapora musi umożliwiać zarządzanie za pomocą interfejsu aplikacji GUI oraz ssh.
   4. Polityka bezpieczeństwa firewall w zakresie kontroli ruchu sieciowego uwzględnia kierunek przepływu pakietów, protokoły i usługi sieciowe, użytkowników i serwery usług, stan połączenia oraz dane aplikacyjne (m.in. obsługuje fragmentację IP, ochronę systemu operacyjnego przed atakami Exploit i DoS).
   5. Zapora wykonuje dynamiczną i statyczną translację adresów NAT. Reguły NAT są generowane automatycznie lub definiowane ręcznie.
   6. Komunikacja pomiędzy modułem zapory sieciowej i modułem zarządzania jest szyfrowana i uwierzytelniona.
   7. Uwierzytelnianie administratorów firewall odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).
   8. Zapora posiada wiele metod uwierzytelniania użytkowników lokalnych i zdalnych (np. uwierzytelnianie przezroczyste gdzie firewall przechwytuje sesję i uwierzytelnia jej użytkownika, uwierzytelnianie za pomocą agenta na stacji użytkownika, uwierzytelniania po połączeniu się z modułem firewall). Baza użytkowników jest przechowywana lokalnie na firewall lub na zewnętrznym serwerze (np. LDAP).
   9. Funkcjonalność zabezpieczeń firewall musi być rozszerzona o mechanizmy ochrony przed intruzami. Mechanizm musi zapewniać co najmniej wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan). Aktualizacja bazy sygnatur ma się odbywać poprzez sieć, automatycznie i na żądanie administratora.
   10. Funkcjonalność zabezpieczeń firewall zawiera moduły pochodzące od producenta zapory:

- moduł kontroli aplikacji sieciowych używanych przez użytkowników wewnętrznych. Identyfikacja aplikacji ma odbywać się w oparciu o bazę danych utrzymywaną przez producenta zapory

- moduł zabezpieczeń IPS wyposażonego w mechanizmy ochrony przez intruzami

- moduł umożliwiający filtrowanie URL. Identyfikacja URL ma odbywać się w oparciu o bazę danych utrzymywaną przez producenta rozwiązania

- moduł ochrony antywirusowej

- moduł Anti – Bot umożliwiający identyfikację stacji roboczych użytkowników zainstalowanych w sieci wewnętrznej, które są zainfekowane agentami botnet.

* 1. Funkcjonalność zabezpieczeń firewall w razie potrzeby może zostać rozszerzona również z użyciem rozwiązań innych producentów. Integracja firewall z zabezpieczeniami innych dostawców odbywa się za pomocą dedykowanych protokołów lub dostarczonego API.
  2. Umożliwia tworzenie sieci VPN w oparciu o standard IPSec/IKE, funkcjonujące w trybie site-site oraz client-site.
  3. Uwierzytelnianie w sieci VPN odbywa się za pomocą certyfikatów cyfrowych wydawanych lokalnie oraz w razie potrzeby przez zewnętrzny urząd certyfikacji.
  4. Zabezpieczenie danych w sieci VPN odbywa się z użyciem mocnych algorytmów kryptograficznych (minimum AES-256).
  5. Zapora musi posiadać obsługę protokołów routingu dynamicznego BGP i OSPF.
  6. Zapora ma możliwość przydziału adresu IP z lokalnej puli lub z serwera DHCP dla zdalnego klienta VPN.
  7. Zapora ma możliwość kierowania całego ruchu sieciowego od i do zdalnego klienta VPN do Internetu przez zaporę i poddania tego ruchu kontroli przez mechanizmy inspekcji uruchomione na zaporze.
  8. Zapora musi zapewniać możliwość jednoczesnego uruchomienia interfejsów pracujących w trybie L2 (bridge, transparent) i w trybie L3 (routing) w ramach tego samego pojedynczego urządzenia fizycznego, pracującego bez uruchamiania wirtualnych ścian ogniowych lub innych funkcji wirtualnych czy obiektów wirtualnych.
  9. Zapora musi posiadać moduł wykrywania intruzów IPS zapewniający wykrywanie i blokowanie ataków w czasie rzeczywistym na bazie sygnatur ataków dostarczanych przez producenta zapory.
  10. Zapora musi umożliwiać kontrolę aplikacji sieciowych używanych przez użytkowników wewnętrznych. Identyfikacja aplikacji musi się odbywać w oparciu o bazę danych aplikacji dostarczaną przez producenta rozwiązania.
  11. Zapora musi umożliwiać przeźroczyste uwierzytelnianie dla użytkowników zalogowanych do Active Directory i na podstawie tego uwierzytelniania przydział do odpowiedniej polityki bezpieczeństwa, czyli po zalogowaniu się do AD, nie jest wymagane ponowne uwierzytelnianie do firewall w celu uzyskania dostępu do zasobów sieciowych, natomiast użytkownikowi są przydzielone prawa dostępu właściwe dla użytkownika lub grupy AD.
  12. Zapora musi umożliwiać filtrowanie ruchu sieciowego pod kątem URL. Identyfikacja URL musi odbywać się w oparciu o bazę dostarczana przez producenta zapory.
  13. Zapora musi umożliwiać wykrywanie, identyfikację i blokowanie w chronionej sieci stacji roboczych będących agentami botnet.
  14. Zapora musi umożliwiać kontrolę antywirusową obsługiwanego ruchu sieciowego, w czasie rzeczywistym, na podstawie bazy sygnatur wirusów dostarczanej przez producenta Zapory.
  15. Umożliwia zestawianie połączeń SSL VPN dla nielimitowanej liczby użytkowników.
  16. Pojedyncze urządzenie zapory musi:

- obsługiwać nielimitowaną licencyjnie liczbę użytkowników,

- posiadać wydajność minimum 35 Gbps ruchu poddawanego inspekcji przez mechanizmy zapory sieciowej (firewall throughput),

- posiadać wydajność minimum 9 Gbps dla ochrony NGFW (NGFW throughput – obejmujący Firewall, Application Control, IPS),

- posiadać wydajność minimum 10 Gbps dla ochrony IPS (IPS throughput),

- posiadać wydajność minimum 20 Gbps dla ruchu szyfrowanego (VPN throughput),

- obsługiwać minimum 8 milionów jednoczesnych sesji/połączeń,

- zapewniać wydajność nawiązywania minimum 300 000 nowych połączeń na sekundę,

- posiadać co najmniej 8 fizycznych interfejsów 10/100/1000 Ethernet z możliwością zainstalowania minimum 8 interfejsów 10 Gbps,

- posiadać dedykowany dla zarządzania port, minimum port konsoli,

- posiadać minimum 2 dyski twarde o pojemności minimum 240 GB każdy,

- posiadać niezbędne komponenty do montażu w szafie rack 19”.

24.27. Gwarancja i wsparcie techniczne producenta w zakresie pomocy przy zgłaszaniu problemów technicznych, dostępu do bazy wiedzy, prawo pobierania poprawek, nowych wersji oprogramowania oraz subskrypcji zabezpieczeń – minimum 3 lata.

1. **System typu Sandbox.**
   1. System Sandbox musi składać się z 2 takich samych urządzeń typu appliance.
   2. Urządzenia typu appliance realizujące funkcje Sandbox muszą umożliwiać zarządzanie z dedykowanego systemu zarządzania.
   3. System zarządzania musi zapewniać zarządzanie dostarczanymi urządzeniami typu appliance w zakresie wszystkich poniższych funkcji:

- centralna konfiguracja polityki bezpieczeństwa dla urządzeń chroniących przed atakami typu Zero-Day i atakami typu APT (Advanced Persistent Threats).

- centralna konfiguracja zasad sandboxingu dokumentów przychodzących.

- centralna konfiguracja zasad rekonstrukcji w formacie bezpiecznym dokumentów przychodzących.

- centralne zarządzanie kontami administratorów i użytkowników.

- centralne monitorowanie i wizualizacja stanu urządzeń realizujących politykę ochrony.

- centralne monitorowanie liczby dokumentów i plików badanych za pomocą procedury sandbox.

- centralne monitorowanie kolejek dokumentów i wydajności ochrony,

- centralne zarządzanie wersjami środowisk wykorzystywanych do procedury sandbox (wersje systemów Windows, typy badanych plików).

- centralne monitorowanie i zarządzanie procedurą aktualizacji środowisk wirtualnych używanych w procedurze sandbox.

* 1. Scentralizowana prezentacja wyników skanowania i badania dokumentów i plików, reportów z procedury sandboxingu z możliwością pobierania dokumentów uznanych za złośliwe do późniejszej analizy.
  2. Wewnętrzny, zintegrowany urząd certyfikacji Certificate Authority pozwalający na zaszyfrowaną i uwierzytelnioną komunikację pomiędzy elementami systemu bezpieczeństwa w zakresie transferu polityki, reguł i logów.
  3. Obsługa systemu zarządzania za pomocą konsoli użytkownika - dedykowanej graficznej konsoli administratora (GUI) działającej pod kontrolą systemu Windows.
  4. Konsola zarządzania z możliwością automatycznej weryfikacji spójności i niesprzeczności polityki bezpieczeństwa.
  5. Uwierzytelnianie administratorów odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych.
  6. Możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkownikami).
  7. Zbieranie i przechowywanie logów bezpieczeństwa do późniejszej analizy .
  8. Wyszukiwanie, filtracja i wyświetlanie logów i zdarzeń zgodnie z szablonami wymaganymi przez administratora (możliwość programowania własnych kwerend).
  9. Zarządzanie integracją z usługami katalogowymi LDAP, w szczególności z Microsoft Active Directory, w zakresie użytkowników i grup w formacie graficznym.
  10. Prezentacja zdarzeń w czasie rzeczywistym w postaci tzw. osi czasowych – zdarzenia mają być grupowane zgodnie z określonymi przez administratora parametrami dla zadanego okresu czasu i wyświetlane zbiorczo w postaci graficznej. Mechanizm ma umożliwiać szybkie sprawdzenie ile zdarzeń określonego typu wydarzyło się w zdefiniowanym przez administratora interwale czasowym.
  11. Graficzna prezentacja zdarzeń pogrupowanych w zależności od kraju pochodzenia źródła.
  12. System raportowania z możliwością powiadamiania administratorów co najmniej za pomocą poczty elektronicznej, SNMP lub definiowanego skryptu uruchamianego w przypadku zaistnienia określonego zdarzenia.
  13. System korelacji informacji o incydentach na podstawie logów.
  14. Pojedyncze urządzenie typu appliance realizujące ochronę typu sandboxing musi podsiadać poniższe funkcje.
      1. Musi chronić przed zagrożeniami zaawansowanymi, atakami typu Zero-Day, atakami typu APT (Advanced Persistent Threats) poprzez sandboxing dokumentów i prewencyjną rekonstrukcję dokumentów.
      2. Ochrona behawioralna – rozpoznawanie oprogramowania złośliwego w fazie exploit poprzez obserwację działania procesora.
      3. Ochrona behawioralna – rozpoznawanie oprogramowania złośliwego w fazie malware poprzez obserwację systemu operacyjnego.
      4. Ochrona ruchu pocztowego - protokół SMTP.
      5. Ochrona ruchu WWW - protokół HTTP.
      6. Ochrona ruchu WWW - protokół HTTPS.
      7. Możliwość pracy autonomicznej w trybie urządzenia sieciowego / zapory (security gateway - ochrona sesji przechodzących przez urządzenie).
      8. Możliwość pracy w trybie prywatnej chmury sandboxingowej na rzecz urządzeń typu firewall.
      9. W trybie urządzenia sieciowego (zapory) możliwość wykrywania i blokowania ruchu wygenerowanego przez oprogramowanie szpiegujące i botnety.
      10. W trybie urządzenia sieciowego (zapory) możliwość wykrywania i blokowania klasycznych wirusów (antywirusowe sygnatury statyczne).
      11. W trybie urządzenia sieciowego (zapory) możliwość definiowania własnych wskaźników zagrożeń IoC (Indicators-of-Compromise) umożliwiających blokowanie wskazanych adresów URL, domen sieciowych, adresów IP, zakresów adresów IP, plików opisanych funkcją MD5, tematów wiadomości pocztowych, adresów źródłowych wiadomości pocztowych, adresów docelowych wiadomości pocztowych, adresów „do wiadomości”.
      12. Możliwość skalowania wydajności poprzez dodawanie urządzeń sandboxingowych do prywatnej chmury.
      13. Ograniczenie wielkości plików badanych w sandboxach nie gorsze niż 100MB.
      14. Praca w warstwie trzeciej (L3) z dynamicznym protokołami routingu.
      15. Praca w warstwie drugiej (L2) jako bridge.
      16. Praca w warstwie drugiej (L2) w trybie monitoringu (mirror port).
      17. Możliwość wykrywania i blokowania zagrożeń (tryby wykrywania lub blokowania).
      18. Tryb chmury prywatnej – działanie bez wysyłania plików przez Internet.
      19. Pojedyncze urządzenie typu appliance realizujące ochronę typu sandboxing musi posiadać:

- redundantne zasilacze oraz redundancję przestrzeni dyskowej co najmniej 1 TB w systemie RAID z możliwością wymiany hot-swap,

- minimum 4 interfejsy 1Gbps oraz 2 interfejsy 10Gbps SFP z modułami SR,,

- minimum 14 wirtualnych środowisk wykonujących operacje sandboxingu zawierających wszystkie wymagane licencje (system operacyjny, produkty MS Office i pozostałe komponenty),

- minimum 1000 Mbps przepustowości w warunkach produkcyjnych (pakiety i sesje charakterystyczne dla ruchu do/z Internetu, liczba transmitowanych plików typowa dla środowiska biurowego),

- wydajność minimum 1300 unikalnych plików poddanych sandboxingowi w ciągu godziny.

* + 1. Gwarancja i wsparcie techniczne producenta w zakresie pomocy przy zgłaszaniu problemów technicznych, dostępu do bazy wiedzy, prawo pobierania poprawek, nowych wersji oprogramowania oraz subskrypcji zabezpieczeń – minimum 3 lata.

1. Wykonawca przeprowadzi instruktarz stanowiskowy dla 3 pracowników Zamawiającego w zakresie obsługi administracyjnej dostarczonych rozwiązań.
2. Wykonawca zrealizuje sesję trwającą 3 dni. W sesji będzie brało udział 3 pracowników Zamawiającego.
3. Sesja instruktarzowa będzie prowadzona w miejscu wskazanym przez Wykonawcę.
4. Wszystkie koszty instruktarzu stanowiskowego pokrywa wykonawca. Dla sesji odbywającej się poza miejscem instalacji systemów Wykonawca pokrywa koszt wyżywienia oraz noclegów.