**Załącznik nr 2**

**FORMULARZ OFERTY** (wzór)

1…......................................................................... ….......................................................

Nazwa wykonawcy/wykonawców składających ofertę wspólną Data sporządzenia

2...................................................................

Wykonawca jest/nie jest płatnikiem VAT

3…................................................................

Nr telefonu

4…................................................................

Nr REGON

5...................................................................

Nr NIP

6.….........................................................................

e-mail do korespondencji

7…................................................................

Nazwisko i imię osoby/osób uprawnionych

do występowania w imieniu wykonawcy

**GMINA MIASTKO**

**ul. Grunwaldzka 1**

**77 - 200 Miastko**

1. Nawiązując do opublikowanego w Biuletynie Zamówień Publicznych (platforma <https://ezamowienia.gov.pl>) ogłoszenia Nr …......................... z dnia …......... …....... 2024 r. o postępowaniu ws. udzielenia zamówienia publicznego na usługę, prowadzonego w trybie podstawowym, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320) o wartości zamówienia mniejszej niż progi unijne określone w przepisach wydanych na podstawie art. 3 ust. 3 przywołanej ustawy, na wykonanie zamówienia **,, Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”** i po zapoznaniu się z warunkami prowadzonego postępowania :
2. **Część I -** **rozbudowa infrastruktury informatycznej urzędu opartą na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN.**
3. Oferujemy i zobowiązujemy się do wykonania zamówienia:

Za cenę ryczałtową w kwocie brutto….........………….………….....................PLN (wraz z podatkiem VAT),

(słownie …............................................................................................................................................),

w tym:

cena netto …………………..PLN

(słownie:……………………………………….……………….………………………………….),

podatek VAT ……………….PLN,

(słownie: ……………………………………………………………….….………………………),

wg obowiązującej stawki w wysokości …..….…..%.

obejmującą:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **LP.** | **Rodzaj zamawianego asortymentu** | **Ilość sztuk/kpl** | **Cena**  **netto** | **VAT** | **Cena brutto** |
| 1. | Serwer I - Dostawa, instalacja i wdrożenie serwerów w celu utworzenia klastra pracy awaryjnej urzędu. Konfiguracja klastra | 3 szt. |  |  |  |
| 2. | Serwer II - Dostawa serwera | 1 szt. |  |  |  |
| 3. | Oprogramowanie i licencje do serwerów | | | | |
| Oprogramowanie | 8 szt. |  |  |  |
| Bezterminowa licencja dostępowa na użytkownika | 110 |  |  |  |
| Bezterminowa licencja dostępowa na urządzenie | 30 |  |  |  |
| 4. | Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników. | 1 szt. |  |  |  |
| 5. | Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych wraz z usługą chmurową | 1 szt. |  |  |  |
| 6. | Wdrożenie oprogramowania do zarządzania infrastrukturą IT na 80 licencji | 1 szt. |  |  |  |
| 7. | Wdrożenie usług domeny do zarzadzania siecią i zasobami komputerowymi | 1 szt. |  |  |  |
| 8. | Przełącznik dystrybucyjny L3 | 1 szt. |  |  |  |
| 9. | Przełączniki sieciowe - Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN | 6 szt. |  |  |  |
| 10. | Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP | 1 szt. |  |  |  |
| 11. | Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych | 5 szt. |  |  |  |
| 12. | Szkolenie ASI tworzenie i administracja sieci VLAN | 1 szt. |  |  |  |
| 13. | Szkolenie ASI tworzenie i administracja serwerami Windows | 1 szt. |  |  |  |
| 14. | Szkolenie ASI z domeny do zarzadzania siecią i zasobami komputerowymi | 1 szt. |  |  |  |
| 15. | Szkolenie ASI Budowa klastra Hyper-V | 1 szt. |  |  |  |
| 16. | Szkolenie z oprogramowania do zarządzania infrastrukturą IT | 1 szt. |  |  |  |

**UWAGA!**

**Zamawiający wymaga załączenia do Formularza ofertowego wykazu oferowanego sprzętu wraz ze szczegółowym opisem technicznym znajdującego się** **w Załączniku nr 2a - Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym - w taki sposób aby Zamawiający mógł jednoznacznie określić szczególne cechy produktu** **oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.**

1. Termin realizacji zamówienia **……. dni kalendarzowych od dnia** (*uzupełnia Wykonawca/termin nieprzekraczalny – nie krótszy 80 dni, nie dłuższy niż 90 dni kalendarzowych*) ;
2. **Cz. II - dostawa oprogramowania do monitorowania infrastrukturą sieci informatycznej i urządzeń dla jednostki podległej oraz dostawa usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy.**
3. Oferujemy i zobowiązujemy się do wykonania zamówienia:

Za cenę ryczałtową w kwocie brutto….........………….…………......PLN (wraz z podatkiem VAT),

(słownie …............................................................................................................................................),

w tym:

cena netto …………………..PLN

(słownie:……………………………………….……………….………………………………….),

podatek VAT ……………….PLN,

(słownie: ……………………………………………………………….….………………………),

wg obowiązującej stawki w wysokości …..….…..%.

obejmującą:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Opis** | **Ilość sztuk/kpl** | **Cena netto** | **VAT** | **Cena brutto** |
| **Lp.** | **Rodzaj zamawianego asortymentu** |
| 1. | Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji dla MOPS | 1 szt. |  |  |  |
| 2. | Usługa zabezpieczenia poczty | 1 szt. |  |  |  |
| 3. | Usługa zabezpieczenia serwisu www na 24 miesiące | 1 szt. |  |  |  |

**UWAGA!**

**Zamawiający wymaga załączenia do Formularza ofertowego wykazu oferowanego oprogramowania wraz ze szczegółowym opisem technicznym znajdującego się** **w Załączniku nr 2b- Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym- w taki sposób aby Zamawiający mógł jednoznacznie określić szczególne cechy produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.**

Termin realizacji zamówienia **……. dni kalendarzowych od dnia** (*uzupełnia Wykonawca/termin nieprzekraczalny – nie krótszy niż 20 dni, nie dłuższy niż 30 dni kalendarzowych*) ;

1. Oświadczamy, że:
2. zapoznaliśmy się z SWZ i nie wnosimy do niej żadnych zastrzeżeń, warunki w niej zawarte akceptujemy bez uwag, zdobyliśmy konieczne informacje do przygotowania oferty;
3. oferowana przez nas cena wykazana w poz. 1 niniejszej oferty obejmuje wszystkie nakłady określone w SWZ i konieczne do wykonania kompletnego dzieła zgodnie z warunkami prowadzonego postępowania oraz przekazania go do użytkowania;
4. uważamy się za związanych niniejszą ofertą przez okres wskazany w swz,

Następujący zakres (cześć) zamówienia powierzymy podwykonawcy/om:

………………………………………………………………………………………………………….

…………………………………………………………………………………………………………

1. Oświadczamy, że w przypadku ujawnienia wad, błędów w wykonanym przedmiocie zamówienia zobowiązujemy się do ich usunięcia na Nasz koszt.
2. Zobowiązujemy się, w przypadku przyznania nam zamówienia, do zawarcia umowy w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty z zastrzeżeniem art. 578 Pzp~~,~~
3. Zobowiązujemy się, w przypadku przyznania nam zamówienia, do zawarcia umowy w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty z zastrzeżeniem art. 578 Pzp;
4. wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.
5. Wykonawca jest (zaznaczyć właściwą opcję)\* :
   * mikroprzedsiębiorstwem
   * małym przedsiębiorstwem
   * średnim przedsiębiorstwem

\*

Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EURO.

Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EURO.

Średnie przedsiębiorstwo:przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EURO.

1. Załącznikami do oferty są:

…........................................................................................................................................................................

…........................................................................................................................................................................

Oferta zawiera …............ ponumerowanych stron.

…....................................................................... …………………………………………………………….

Miejscowość i data Podpis wykonawcy/osoby upoważnionej

do występowania w imieniu wykonawcy

Załącznik 2a

**Wykaz oferowanego sprzętu wraz z szczegółowym opisem technicznym**

Cz.I - rozbudowa infrastruktury informatycznej urzędu opartą na dostawie sprzętu wraz z instalacją, montażem i przeniesieniem danych z obecnej sieci informatycznej oraz wdrożenie oprogramowania do zarządzania siecią IT wraz z konfiguracją sieci VLAN.

**UWAGA!**

Zamawiający wymaga dołączenia wykazu oferowanego sprzętu do formularza ofertowego. W pozycji parametry oferowane należy umieścić opis techniczny umożliwiający Zamawiającemu jednoznaczne określenie szczególnych cech produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.

**W przypadku nie dołączenia wymienionego powyżej wykazu do formularza oferty oferta podlega odrzuceniu jako niezgodna z zapisami swz.**

1. **Dostawa, instalacja i wdrożenie klastra pracy awaryjnej urzędu składającego się z 3 serwerów wraz z systemem operacyjnym.**

Zaoferowane serwery musza spełniać minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Minimalne parametry wymagane** | **Parametry oferowane** |
|  | **Obudowa** | Do szafy Rack 19", wysokość 1U, z zestawem szyn do mocowania w szafie; |  |
|  | **CPU** | Zainstalowane 2 procesory w architekturze x86, dokładnie 8-rdzeniowe, o TDP nie większym niż 165W. Wynik wydajności procesora instalowanego w oferowanym serwerze wynoszący min. 178 punktów w teście SPECrate®2017\_int\_base, dla konfiguracji dwuprocesorowej. Wynik testu przeprowadzony dla oferowanego modelu serwera oraz zgodnego modelu procesora dostępny na stronie <https://www.spec.org/>; |  |
|  | **Płyta główna** | * Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; * Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; * Wyposażona w moduł zabezpieczeń zgodny z TPM 2.0; * Posiadająca 32 sloty DIMM na pamięć DDR5, obsługująca do 8TB pamięci RAM; |  |
|  | **Pamięć RAM** | * Zainstalowane minimum 128GB pamięci RAM, pracującej w oferowanej konfiguracji z częstotliwością min. 4800MHz, w modułach o pojemności 32GB każdy; |  |
|  | **Protekcja pamięci RAM** | * Memory mirroring, ECC, Advanced ECC lub SDDC; |  |
|  | **GPU** | * Wbudowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz; |  |
|  | **Zatoki dyskowe** | * Serwer wyposażony w 8 zatok dyskowych hot-plug 2.5” umożlwiających instalację dysków SSD/HDD z interfejsem SATA/SAS; * Serwer wyposażony w kontroler sprzętowy RAID pozwalający na obsługę RAID 0,1,10,5; * Serwer umożlwiający rozbudowę o 2 dyski M.2 SSD NVMe o pojemności min. 960GB działające ze sprzętowym RAID 1; |  |
|  | **Zasilanie** | * Dwa zasilacze o mocy min. 1000W z certyfikatem Titanium. |  |
|  | **Karty sieciowe** | * Karta Ethernet posiadająca 2 porty 10 GbE BASE-T (RJ-45) * Karta Ethernet posiadająca 2 porty 10/25GBE SFP28 |  |
|  | **Sloty PCIe** | * Serwer posiadający 2 sloty PCIe generacji 4.0 dostępne do instalacji kart rozszerzeń bez konieczność rekonfiguracji serwera; * Możliwość rozbudowy oferowanego serwera o 2 karty GPU o pamięci podręcznej min. 16GB oraz wydajności 9 TFLOPS dla obliczeń Tensor-Float 32 każda. |  |
|  | **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.0, 1x USB 2.0, 1x VGA * z tyłu obudowy: 3x USB 3.0, 1x VGA * wewnętrzne: 1 x USB 3.0 |  |
|  | **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |  |
|  | **Zarządzanie** | Serwer wyposażony w moduł zarządzający posiadający dedykowany port 1GbE Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł umożliwia:   * monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe * dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub * dostęp do karty możliwy: * z poziomu przeglądarki webowej (GUI) * z poziomu linii komend (SSH lub IPMI) * wbudowane narzędzia diagnostyczne * zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego * obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie * wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników * przesyłanie alertów poprzez e-mail oraz SNMP * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) * zdalna aktualizacja oprogramowania (firmware) * możliwość równoczesnej obsługi przez min. 2 administratorów * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) * możliwość instalacji karty Micro SD udostępniającej min. 4GB przestrzeni na potrzeby karty zarządzającej * Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS * Możliwość monitorowania i zarządzania grupą do 200 serwerów z poziomu kontrolera zarządzania pojedynczego serwera   Serwer wyposażony w wbudowany panel LCD umieszczony na froncie obudowy i pozwalający na wyświetlenie informacji o: stanie serwera, konfiguracji sieciowej karty zarządzającej, zasilaniu, temperaturze.  Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS.  Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych. |  |
|  | **Funkcje zabezpieczeń** | * Czujnik otwarcia obudowy; * TPM 2.0; |  |
|  | **Urządzenia hot- swap** | Dyski twarde, zasilacze, wentylatory. |  |
|  | **Gwarancja** | * 36 miesięcy wsparcia technicznego realizowanego w trybie on-site (naprawa na w miejscu instalacji) lub poprzez wysyłkę części; * Usługa wsparcia technicznego świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń; |  |
|  | **Inne** | * Serwer wyprodukowany zgodnie z normą ISO-9001 oraz ISO14001; * Elementy, z których zbudowane są serwery są produktami producenta tych serwerów lub są przez niego certyfikowane oraz są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; * Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją możliwa przy użyciu dedykowanych dla danego modelu serwera komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; * Serwer fabrycznie nowy z oficjalnego kanału dystrybucyjnego w Polsce; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia |  |

1. **Serwer II - Dostawa serwera**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Minimalne parametry wymagane** | **Parametry oferowane** |
|  | **Obudowa** | * Do szafy Rack 19", wysokość 1U, z zestawem szyn do mocowania w szafie; |  |
|  | **CPU** | * Zainstalowany 1 procesor w architekturze x86, 16-rdzeniowy, o TDP nie większym niż 150W. Wynik wydajności procesora instalowanego w oferowanym serwerze wynoszący min. 267 punktów w teście SPECrate®2017\_int\_base, dla konfiguracji dwuprocesorowej. Wynik testu przeprowadzony dla oferowanego modelu serwera oraz zgodnego modelu procesora dostępny na stronie <https://www.spec.org/>; * Możliwość rozbudowy serwera o drugi procesor tego samego typu co zainstalowany; |  |
|  | **Płyta główna** | * Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera; * Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje; * Wyposażona w moduł zabezpieczeń zgodny z TPM 2.0; * Posiadająca 32 sloty DIMM na pamięć DDR5, obsługująca do 8TB pamięci RAM; |  |
|  | **Pamięć RAM** | * Zainstalowane minimum 64GB pamięci RAM, pracującej w oferowanej konfiguracji z częstotliwością min. 4400MHz, w modułach o pojemności 32GB każdy; |  |
|  | **Protekcja pamięci RAM** | * Memory mirroring, ECC, Advanced ECC lub SDDC; |  |
|  | **GPU** | * Wbudowana karta graficzna osiągająca rozdzielczość 1920x1200 przy 60 Hz; |  |
|  | **Zatoki dyskowe** | * Serwer wyposażony w 4 zatoki dyskowych hot-plug 3.5” umożlwiające instalację dysków SSD/HDD z interfejsem SATA/SAS; * Serwer wyposażony w kontroler sprzętowy RAID pozwalający na obsługę RAID 0,1,10,5; * Serwer umożlwiający rozbudowę o 2 dyski M.2 SSD NVMe o pojemności min. 960GB działające ze sprzętowym RAID 1; |  |
|  | **Nośniki danych** | * Serwer wyposażony w 2 dyski SSD hot-plug, dedykowane do serwerów, o pojemności 960GB każdy; |  |
|  | **Zasilanie** | * Dwa zasilacze o mocy min. 1000W z certyfikatem Titanium. |  |
|  | **Karty sieciowe** | * Karta Ethernet posiadająca 2 porty 10 GbE BASE-T (RJ-45) |  |
|  | **Sloty PCIe** | * Serwer posiadający 1 sloty PCIe generacji 4.0 dostępny do instalacji kart rozszerzeń bez konieczność rekonfiguracji serwera; |  |
|  | **Dodatkowe porty** | * z przodu obudowy: 1x USB 3.0 * z tyłu obudowy: 3x USB 3.0, 1x VGA * wewnętrzne: 1 x USB 3.0 |  |
|  | **Chłodzenie** | Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |  |
|  | **Zarządzanie** | Serwer wyposażony w moduł zarządzający posiadający dedykowany port 1GbE Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web. Moduł umożliwia:   * monitorowanie podzespołów serwera: temperatura, zasilacze, * wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe * dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub * dostęp do karty możliwy: * z poziomu przeglądarki webowej (GUI) * z poziomu linii komend (SSH lub IPMI) * wbudowane narzędzia diagnostyczne * zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego * obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie * wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników * przesyłanie alertów poprzez e-mail oraz SNMP * obsługa zdalnego serwera logowania (remote syslog) * wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów * monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji * konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) * zdalna aktualizacja oprogramowania (firmware) * możliwość równoczesnej obsługi przez min. 2 administratorów * wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) * możliwość instalacji karty Micro SD udostępniającej min. 4GB przestrzeni na potrzeby karty zarządzającej * Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS * Możliwość monitorowania i zarządzania grupą do 200 serwerów z poziomu kontrolera zarządzania pojedynczego serwera   Możliwość zarządzania – monitoring parametrów pracy i konfiguracja najważniejszych komponentów - z poziomu urządzania mobilnego przy użyciu dedykowanej aplikacji dostępnej na Android i/lub iOS.  Oprogramowanie diagnostyczne producenta serwera (lub wbudowana funkcja karty zarządzającej) posiadające funkcjonalność predykcji awarii wszystkich kluczowych komponentów serwera: procesorów, pamięci RAM, dysków wewnętrznych HDD/SSD/M.2 SSD, wentylatorów, zasilaczy, kontrolerów dyskowych. |  |
|  | **Funkcje zabezpieczeń** | TPM 2.0; |  |
|  | **Urządzenia hot- swap** | Dyski twarde, zasilacze, wentylatory. |  |
|  | **Gwarancja** | * 36 miesięcy wsparcia technicznego realizowanego w trybie on-site (naprawa na w miejscu instalacji) lub poprzez wysyłkę części; * Usługa wsparcia technicznego świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń; |  |
|  | **Inne** | * Serwer wyprodukowany zgodnie z normą ISO-9001 oraz ISO14001; * Elementy, z których zbudowane są serwery są produktami producenta tych serwerów lub są przez niego certyfikowane oraz są objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; * Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją możliwa przy użyciu dedykowanych dla danego modelu serwera komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera; * Serwer fabrycznie nowy z oficjalnego kanału dystrybucyjnego w Polsce; * Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanych serwerów, nawet po wygaśnięciu 3-letniego okresu wsparcia |  |

1. **Oprogramowanie i licencje do serwerów;**

Wymagane jest dostarczenie i wgranie oprogramowania oraz licencji na dostarczonych w ramach postępowania serwerach.

Oprogramowanie dla serwerów oraz licencje muszą spełniać poniższe minimalne parametry:

|  |  |  |
| --- | --- | --- |
| **Opis** | **Minimalne parametry wymagane** | **Parametr oferowany** |
| **Oprogramowanie – 8 szt.** | * System operacyjny dedykowany do serwerów w wersji komercyjnej o zamkniętym kodzie źródłowym. * System operacyjny powinien być dostarczony w najnowszej dostępnej wersji od producenta. * System operacyjny nowy, dostarczony ze wszystkimi atrybutami legalności. * Licencja musi mieć możliwość przenoszenia na inne serwery fizyczne. * Licencja nieograniczona czasowo ani funkcjonalnie. * Licencja wieczysta dla oferowanej konfiguracji serwerów. |  |
| **Bezterminowa licencja dostępowa na użytkownika – 110 licencji** | * Dostarczona licencja musi być fabrycznie nowa. * Licencja musi być najnowszą wersją, możliwą do nabycia od producenta. * Licencja nieograniczona czasowo ani funkcjonalnie. * Dostarczona licencja musi posiadać cechy/atrybuty legalności. |  |
| **Bezterminowa licencja dostępowa na urządzenie – 30 licencji,** | * Dostarczona licencja musi być fabrycznie nowa. * Licencja musi być najnowszą wersją, możliwą do nabycia od producenta. * Licencja nieograniczona czasowo ani funkcjonalnie. * Dostarczona licencja musi posiadać cechy/atrybuty legalności. |  |

1. **Macierz - Dostawa, instalacja, konfiguracja macierzy z klastrem pracy awaryjnej, Przeniesienie danych z dotychczasowych nośników. – 1 szt.**

Dostarczona macierz powinna spełniać minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Opis przedmiotu zamówienia/ parametry wymagane** | **Parametr oferowany** |
| 1. | Obudowa | instalacja w szafie technicznej typu RACK 19”,  Wysokość max. 2U. |  |
| 2. | Kontrolery dyskowe | * Min. 2 kontrolery macierzowe pracujące w trybie Symmetrical Active-Active/Mesh Active-Active, to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing) nawet dla pojedynczego LUN. Dla utworzonego jednego LUN operacje I/O muszą być realizowane jednocześnie przez porty w obu kontrolerach, a generowane obciążenie (IOPS oraz Bandwidth) mają być rozłożone dla pary kontrolerów w stosunku 50/50 +/- 10%. * W przypadku zaoferowania większej ilości kontrolerów obciążenie ma być rozłożone proporcjonalnie na wszystkie kontrolery.   Kontrolery muszą pozwalać na udostępnianie zasobów protokołami plikowymi oraz blokowymi.  Komunikacja pomiędzy oferowanymi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband.  Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze więcej niż 2 kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego. |  |
| 3. | Możliwość rozbudowy | Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 6 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązań opartych o wirtualizator.  Macierz wyłącznie do obsługi modułów pamięci NVME i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych.  Urządzenie musi umożliwiać dynamiczną zmianę rozmiaru woluminów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się w danym LUN.  Urządzenie musi umożliwiać rozbudowę przestrzeni dyskowej o pojedynczy dysk oraz pojedynczą półkę dyskową z możliwością rozszerzenia puli dyskowej o dodany dysk/półkę bez konieczności migracji danych ani zatrzymywania pracy macierzy. |  |
| 4. | Wymagana przestrzeń | Całkowita pojemność surowa RAW urządzenia musi wynosić minimum 23 TB i być zbudowana tylko i wyłącznie za pomocą dysków SSD NVMe/modułów NVMe o maksymalnej pojemności pojedynczego modułu 4 TB.  Macierz musi umożliwiać rozbudowę do co najmniej 100 sztuk oferowanego typu modułów pamięci NVMe, bez wymiany lub dodawania kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek dyskowych oraz kart z interfejsami i modułów NVMe).  Moduły NVMe muszą posiadać redundantne interfejsy PCIe Gen 4. |  |
| 5. | Procesory/Pamięć Cache | Każdy kontroler macierzy musi być oparty o wielordzeniowe procesory, minimum dwadzieścia rdzeni łącznie na kontroler.  Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |  |
| 6. | Zabezpieczenie danych | Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.  Urządzenie musi obsługiwać poziomy RAID5, RAID6 lub RAID DP (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare), oraz RAID 10. |  |
| 7. | Dostępne interfejsy | Macierz musi posiadać:   * minimum 8 portów 25 Gb/s lub 4 porty 100GB/s obsługujących protokół NVMe over RoCE. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28,QSFP28), wymaga się ich dostarczenia wraz z urządzeniem; * minimum 2 wkładki jednomodowe ze złączem LC oraz komplet patchcordów jednomodowych o długości 50cm * minimum 8 portów 10Gb/s na całą macierz. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+/SFP28), wymaga się ich dostarczenia wraz z urządzeniem; * minimum 8 wkładek multimodowych 10Gb/s ze złączem LC oraz komplet patchcordów multimodowych o długości 50cm   W oferowanej konfiguracji portów macierz musi posiadać pełną możliwość rozbudowy do wymaganej ilości modułów pamięci bez usuwania żadnego z interfejsów. |  |
| 8. | Brak pojedynczego punktu awarii | Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy. |  |
| 9. | Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (Thin Provisioning) | Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation).  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. |  |
| 10. | Protokoły dostępu do danych | Wymagane wsparcie dla NVMe over RoCE, iSCSI, NFS, CIFS. Wymagana obsługa protokołów plikowych minimum:  - CIFS (minimum SMB 2.0, SMB 2.1, SMB 3.0, oraz SMB 3.1.1)  - NFS (minimum NFSv3, NFSv4.0 oraz NFSv4.1).  Dla zasobów udostępnianych plikowo macierz musi posiadać funkcjonalność definiowania polityk umożliwiających limitowanie ilości plików w danym katalogu oraz jego maksymalnego rozmiaru. Nie dopuszcza się realizacji funkcjonalności dostępu plikowego za pomocą dodatkowych/zewnętrznych urządzeń. Funkcjonalność ta musi być wbudowana w oprogramowanie zainstalowane w kontrolerach urządzenia.  Dla zasobów plikowych macierz musi posiadać możliwość uruchomienia replikacji w trybach synchronicznym oraz asynchronicznym.  Jeśli obsługa protokołów plikowych wymaga dodatkowej licencji, to nie jest wymagane jej dostarczenie wraz z urządzeniem. |  |
| 11. | WORM | Dla zasobów plikowych macierz musi umożliwiać skonfigurowanie funkcji Write Once Read Many (WORM) dla utworzonego systemu plików. Każdy plik objęty ochroną WORM musi przechodzić w stan tylko do odczytu natychmiast po zapisaniu na macierzy. W stanie tylko do odczytu plik można odczytać, ale nie można go usunąć, zmodyfikować ani zmienić jego nazwy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie nie jest wymagane wraz z urządzeniem. |  |
| 12. | Snapshoty | Urządzenie musi umożliwiać utworzenie 1000 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 4000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write).  Rozwiązanie musi umożliwiać tworzenie grup spójności, które gwarantują spójne kopiowanie, odtwarzanie i odświeżanie wielu wolumenów naraz tj. tworzenie kopii zapasowej wielu LUNów jednocześnie.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem.  Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii).  Dla zasobów plikowych macierz musi umożliwiać wykonywanie kopii migawkowych systemu plików z którego dane udostępniane są protokołem CIFS. Po wykonaniu kopii zmiany danych lub zapisy w systemie plików nie będą miały wpływu na dane kopii migawkowej. Musi istnieć możliwość zabezpieczenia kopii przed modyfikacją i usunięciem przez zadany okres czasu. |  |
| 13. | Funkcje kopiujące | Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. |  |
| 14. | Redukcja danych | Macierz musi mieć funkcjonalność deduplikacji i kompresji danych w trybie in-line zarówno dla danych blokowych jak i systemu plików. Administrator musi mieć możliwość wyłączenia mechanizmów redukcji danych dla poszczególnych woluminów LUN. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. |  |
| 15. | Replikacja danych | Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach NVMe over RoCE lub IP bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. |  |
| 16. | Klaster wysokiej dostępności | Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po NVMe over RoCE lub IP pomiędzy 2 macierzami dostarczonymi w tym postępowaniu. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać klastrowanie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. |  |
| 17. | Priorytety zadań | Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane wraz z urządzeniem. |  |
| 18. | Kompatybilność | Model oferowanej macierzy musi znajdować się na oficjalnej liście zgodności VMware (dostępnej na stronie <https://www.vmware.com/resources/compatibility/search.php>).  Rozwiązanie musi wspierać integrację w zakresie technologii konteneryzacji poprzez posiadanie dedykowanego sterownika Container Storage Interface (CSI). |  |
| 19. | Licencje | Macierz musi być dostarczona z licencjami wymaganymi do instalacji kontrolerów z dyskami, oraz uruchomienia mechanizmów wymaganych w OPZ. |  |
| 20. | Wielościeżkowość | Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows Server 2019 oraz 2022, Vmware 8.0 i nowszych. |  |
| 21. | Zasilanie | Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap. |  |
| 22. | Zarządzanie macierzą | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów NVME. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI z co najmniej 2 lat wstecz. Macierz musi umożliwiać monitorowanie oraz przeglądanie danych historycznych z podziałem dla każdego z LUN dla min. operacji: -% trafień w cache do odczytu oraz zapisu  -IOPS  -średni czas odpowiedzi dla odczytu danych  -średni czas odpowiedzi dla zapisu danych  -przepustowość „Bandwidth” dla operacji odczytu  -przepustowość „Bandwidth” dla operacji zapisu  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.  Rozwiązanie musi udostępniać interfejs REST API w celu uruchamiania skryptów oraz SNMP do komunikacji z zewnętrznymi narzędziami monitorującymi. |  |
| 23. | Serwisowalność | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.  Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.  Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną. |  |
| 24. | Gwarancja, wsparcie serwisowe | 1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta na terenie RP. 2. Macierz dyskowa musi zostać objęta **minimum 60 miesięcznym okresem gwarancji** (parametr oceniany) w trybie **on-site** z gwarantowanym czasem reakcji w ciągu 60 min od momentu zgłoszenia usterki. 3. Uszkodzone dyski po awarii pozostają u Zamawiającego bez konieczności zwrotu do serwisu/producenta. 4. Zgłoszenia usterek muszą być akceptowane zarówno drogą email (w ofercie należy podać dedykowany adres email do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych, o podwyższonej płatności itp.). 5. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. 6. Usługi gwarancyjne muszą być świadczone przez organizację serwisową producenta sprzętu posiadającą certyfikat ISO co najmniej 9001:2015. 7. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:  * możliwość pobierania najnowszego firmware; * dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; * dostęp do centrum pomocy technicznej producenta; * otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; * otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy |  |

1. **Dostawa i wdrożenie oprogramowania do wykonywania kopii zapasowych wraz z usługą chmurową**

Minimalne parametry techniczne:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis przedmiotu zamówienia/ parametry wymagane** | **Parametr oferowany** |
| 1. I | Wymagania minimalne: |  |
| 1. 1 | Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji |  |
| 1. a | Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012 |  |
| 1. b | Vmware vSphere min. w wersjach v5.5-7.0.3 |  |
| 1. c | Nutanix AHV 5.15, 5.20 (LTS) |  |
| 1. d | Maszyny fizyczne: Windows Server 2022, 2019, 2016, 2012R2, 2012 |  |
| 1. e | Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams) |  |
| 1. 2 | Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V |  |
| 1. 3 | Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia: |  |
| 1. a | na serwerze Windows lub Linux |  |
| 1. b | jako maszyna wirtualna Vmware |  |
| 1. c | jako maszyna wirtualna Amazon |  |
| 1. d | na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital |  |
| 1. 4 | Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS |  |
| 1. 5 | Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania |  |
| 1. 6. | Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji). |  |
| 1. II | Licencjonowanie – wymaga się dostarczenia min. 6 licencji |  |
| 1. 1 | Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności |  |
| 1. 2 | Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska |  |
| 1. 3 | W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania |  |
| 1. 4 | W ramach dostawy wymagane jest dostarczenie licencji na ochronę X gniazd procesorów w hostach Vmware lub Hyper-V |  |
| 1. 5 | W ramach dostawy wymagane jest dostarczenie licencji na ochronę X maszyn fizycznych z systemem operacyjnym Windows Server lub Linux (w wersji serwerowej) |  |
| 1. 6 | W ramach dostawy wymagane jest dostarczenie licencji na ochronę X maszyn fizycznych z systemem operacyjnym Windows 10 Pro lub Ubuntu Desktop |  |
| 1. 7 | Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska |  |
| 1. III | Ochrona danych |  |
| 1. 1 | Oprogramowanie musi posiadać funkcje backupu i replikacji: |  |
| 1. a | Backup maszyn wirtualnych Vmware |  |
| 1. b | Replikacja maszyn wirtualnych Vmware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu |  |
| 1. c | Backup maszyn wirtualnych Hyper-V |  |
| 1. d | Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu |  |
| 1. e | Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych |  |
| 1. f | Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie |  |
| 1. g | Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu |  |
| 1. h | Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym |  |
| 1. i | "Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych |  |
| 1. j | Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania |  |
| 1. k | Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji |  |
| 1. l | Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach |  |
| 1. IV | Optymalizacja wykorzystania miejsca na dane |  |
| 1. 1 | Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych: |  |
| 1. a | Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane |  |
| 1. b | Kompresja backupu, w tym konfigurowalny stopień kompresji |  |
| 1. c | Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne |  |
| 1. V | Spójność danych |  |
| 1. 1 | Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych: |  |
| 1. a | Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux |  |
| 1. b | Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu |  |
| 1. c | Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: |  |
|  | Microsoft Exchange 2013, 2016, 2019 |  |
|  | Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022 |  |
| 1. d | Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki |  |
| 1. e | Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V |  |
| 1. f | Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania |  |
| 1. g | Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji |  |
| 1. VI | Przywracanie danych |  |
| 1. 1 | Oprogramowanie musi posiadać poniższe funkcje: |  |
| 1. a | Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji |  |
| 1. b | Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) |  |
| 1. c | Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej) |  |
| 1. d | Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): |  |
|  | Microsoft Exchange |  |
|  | MS Active Directory |  |
|  | MS SQL |  |
| 1. e | Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie. |  |
| 1. VII | Wydajność |  |
| 1. 1 | Oprogramowanie do backupu musi pozwalać na: |  |
| 1. a | Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT |  |
| 1. b | Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych |  |
| 1. c | Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN |  |
| 1. d | Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci |  |
| 1. e | Wsparcie dla urządzeń oferujących dodatkową deduplikację danych |  |
|  | Zarządzanie |  |
| 1. 1 | Oprogramowanie musi pozwalać na następujące formy zarządzania: |  |
| 1. a | Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych |  |
| 1. b | Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej |  |
| 1. c | Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania |  |
| 1. d | Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport. |  |
| 1. e | Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji |  |

usługa odmiejscowionej kopii zapasowej danych w chmurze min. 2TB, która zapewni regularne tworzenie, przechowywanie oraz odtwarzanie kopii zapasowych danych Zamawiającego. Usługa ta ma na celu zabezpieczenie danych przed utratą, zapewniając dostępność, integralność oraz bezpieczeństwo informacji zgodnie z obowiązującymi normami i przepisami prawnymi.

Kopia w chmurze będzie służyła do przechowywania strategicznych dokumentów i baz danych Zamawiającego.

Minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | **Przedmiot zamówienia** | **Minimalne parametry wymagane** | **Parametr oferowany** |
|  | Rodzaj chmury | Usługa musi być realizowana w chmurze prywatnej, z możliwością skalowania przestrzeni dyskowej zgodnie z potrzebami Zamawiającego. |  |
|  | Częstotliwość wykonywania kopii zapasowych: | Kopie zapasowe muszą być wykonywane regularnie, z częstotliwością co najmniej raz dziennie.  Możliwość ustawienia harmonogramu tworzenia kopii zapasowych (np. codziennie, co godzinę, co tydzień, w zależności od krytyczności danych). |  |
|  | Szyfrowanie: | Dane muszą być szyfrowane w trakcie transferu (end-to-end encryption) oraz w spoczynku (encryption at rest) z użyciem algorytmu szyfrowania co najmniej AES-256. |  |
|  | Przestrzeń dyskowa: | Usługa musi umożliwiać elastyczne zarządzanie przestrzenią dyskową, z możliwością zwiększenia pojemności bez przerw w działaniu usługi. |  |
|  | Czas przechowywania kopii: | Przechowywanie kopii zapasowych przez minimum 30 dni z możliwością rozszerzenia tego okresu na żądanie Zamawiającego.  Możliwość ustawienia polityk retencji (usuwania starszych kopii zapasowych po określonym czasie). |  |
|  | Funkcjonalności usługi | Usługa musi zapewniać automatyczne tworzenie kopii zapasowych zgodnie z ustalonym harmonogramem, bez konieczności ręcznego zarządzania procesem przez użytkownika.  Zamawiający musi mieć zapewniony bezpieczny i szybki dostęp do kopii zapasowych w celu ich odtworzenia w razie awarii, a także możliwość przeglądania i zarządzania kopii zapasowych przez panel zarządzania.  System musi generować raporty oraz powiadomienia dotyczące statusu kopii zapasowych, w tym powiadomienia o błędach, sukcesach oraz stanie przestrzeni dyskowej. |  |
|  | Wymagania dotyczące bezpieczeństwa | -Wymaga się, aby usługodawca spełniał najwyższe standardy bezpieczeństwa w zakresie ochrony danych, zgodnie z normami ISO/IEC 27001 lub równoważnymi.  -Usługa musi spełniać wymogi przepisów prawa o ochronie danych osobowych, w tym RODO.  -Możliwość przeprowadzania regularnych audytów bezpieczeństwa oraz dostępu do logów z działań związanych z tworzeniem i odtwarzaniem kopii zapasowych. |  |
|  | Gwarancja jakości | Usługa musi być świadczona zgodnie z uzgodnionymi parametrami SLA, zapewniającymi m.in. określony czas reakcji na awarie, czas odtworzenia danych oraz dostępność usługi. |  |
|  | Okres realizacji zamówienia | Okres świadczenia usługi wynosi 18 miesięcy. |  |

1. **Dostawa oprogramowania wraz z instalacją i wdrożeniem oprogramowania do zarządzania infrastrukturą IT dla 80 licencji wieczystych:**

Minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Minimalne parametry wymagane** | **Parametr oferowany** |
| 1. | Oprogramowanie: | 1. Budowa modułowa, 2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. 3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. 4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych 5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania |  |
| 2. | Monitorowanie danych użytkownika: | 1. historia aktywności 2. polityka korzystania z Internetu i aplikacji 3. dostęp do zewnętrznych nośników danych, 4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodne z RODO bez konieczności usunięcia informacji o stacji roboczej, 5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO, 6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników, 7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia, 8. konfiguracja haseł użytkownika 9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej |  |
| 3. | Funkcjonalności: | Oprogramowanie obsługuje m.in. 6 funkcjonalności:   1. Monitorowanie infrastruktury, 2. Inwentaryzacja sprzętu i oprogramowania, 3. Monitorowanie aktywności użytkowników, 4. Realizacja zdalnej pomocy użytkownikom, 5. Ochrona danych przed wyciekiem, 6. Wsparcie zarządzania czasem i analizowanie aktywności użytkowników |  |
| 4. | Monitorowanie infrastruktury: | 1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping, 2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją, 3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów, 4. Serwery pocztowe:  * program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, * program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, * program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa  1. Monitorowanie serwerów WWW i adresów URL 2. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 3. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail 4. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 5. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 6. Monitoringu routerów i przełączników wg:  * zmian stanu interfejsów sieciowych * ruchu sieciowego * podłączonych stacji roboczych – graficzna prezentacja panelu switcha * ruchu generowanego przez podłączone do portów stacje robocze  1. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie, 2. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 3. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 4. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 5. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy, 6. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera. 7. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 8. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. 9. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 |  |
| 5. | Inwentaryzacja sprzętu i oprogramowania, | 1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów, 2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu 5. Zbieranie informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiejkolwiek zmiany na urządzeniu 7. Możliwość odczytania numeru seryjnego (klucze licencyjne). 8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.   *Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:*   1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 2. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 3. tworzenia powiązań między zasobami a urządzeniami, 4. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory ), wskazywanie osób odpowiedzialnych, 5. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 6. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, 7. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 8. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 9. masową edycję atrybutów zasobów, 10. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 11. importu danych z zewnętrznego źródła (.CSV), 12. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 13. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 14. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 15. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 16. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 17. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 18. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 19. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 20. archiwizacji i porównywania audytów zasobów, 21. tworzenia kodów kreskowych dla zasobów, 22. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 23. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 24. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 25. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 26. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   *Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:*   1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji. 4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji, 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. |  |
| 6. | Monitorowanie aktywności użytkowników: | 1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, 3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, 4. Informacja o edytowanych przez użytkownika dokumentach, 5. Historia pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, 9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail. 10. Wykrywanie podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy. 11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 12. Wyszczególnienie podejrzanej aktywności w raportach. 13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności. 14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). 16. Blokowania ruchu na wskazanych portach TCP/IP, 17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 18. Prowadzenie rejestru naruszeń blokad, 19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, 20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. |  |
| 7. | Realizacja zdalnej pomocy użytkownikom | 1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika, 2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów. 3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów.   Czat powinien pozwalać na:   1. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 2. rozmowy między „zwykłymi” użytkownikami 3. przesyłanie plików między rozmówcami w trybie online 4. tworzenie pokojów tematycznych, rozmów grupowych 5. oznaczanie kontaktów jako „ulubionych” na liście kontaktów 6. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, 7. Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów.   Moduł pomocy zdalnej powinien umożliwiać:   1. pobieranie listy użytkowników z Active Directory, 2. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 3. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, 4. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń, 5. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 6. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 7. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 8. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 9. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 10. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 11. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 12. eksportowania listy zgłoszeń do plików CSV i XLSX, 13. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 14. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 15. wykonywanie operacji na wielu zgłoszeniach równocześnie, 16. dołączanie załączników do zgłoszeń, 17. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 18. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 19. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 20. zrzuty ekranowe (podgląd pulpitu), 21. zdalną modyfikację rejestrów, 22. dystrybucję oprogramowania przez Agenty, 23. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 24. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 25. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 26. planowanie nieobecności pracowników helpdesk, 27. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 28. generowanie raportów obsługi helpdesk, 29. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 30. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 31. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików. |  |
| 8. | Ochrona danych przed wyciekiem | Blokowanie urządzeń i nośników danych:   1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender 11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.   Zarządzanie prawami dostępu do urządzeń:   1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.   Audyt operacji na plikach na urządzeniach przenośnych:   1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. 3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 4. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. |  |
| 9. | Zarządzanie czasem i analizowanie aktywności użytkowników | 1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym. 2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. 3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania.   Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym.   1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 2. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 3. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 4. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 5. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 6. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 7. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 8. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 9. Wskaźnik czasu poświęconego na aktywność produktywną. 10. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 11. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 12. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów. |  |
| 10. | Gwarancja, wsparcie serwisowe | 1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru 2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania. 3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania 4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów). 5. Świadczenie przez Producenta pomocy w formie sesji zdalnych. 6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy. 7. Możliwość przedłużenia wsparcia o kolejny rok 8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły |  |

1. **Dostawa i instalacja i konfiguracja przełącznika dystrybucyjnego (zwany powyżej L3) – 1 szt.**

Minimalne parametry techniczne:

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (Wymagane minimalne)** | **Parametr oferowany** |
| Przełącznik posiada: | 1. min. 48 portów 1/10/25GE SFP28 bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego 2. min. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps 3. Pamięć systemu min. 24 GB 4. Dysk SSD min. 64 GB |  |
| Parametry wydajnościowe: | 1. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 2. Obsługiwana łączna przepływność (pasmo) min. 3,6 Tbps 3. Obsługiwana łączna przepustowość pakietowa przełącznika min. 1,6 bpps 4. opóźnienie przełączania pakietów nie większe niż 2 µs . |  |
| Funkcjonalność warstwy L2: | 1. Trunking IEEE 802.1Q VLAN; 2. Wsparcie dla min. 3967 sieci VLAN; 3. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN 4. Wsparcie sprzętowe dla minimum 256 tysięcy adresów MAC 5. IEEE 802.1s Multiple Spanning Tree (MST) 6. Statyczny i dynamiczny NAT 7. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree 8. Internet Group Management Protocol (IGMP) |  |
| Funkcjonalność warstwy L3 | 1. Sprzętowe przełączanie pakietów w warstwie L3 2. Routing w oparciu o trasy statyczne 3. Routing w oparciu o OSPF, BGP 4. Wsparcie sprzętowe dla minimum 896 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP 5. Wsparcie dla IPv4 multicast w oparciu o protokół PIM-SM Sparse Mode I tryb SSM (Source Specific Multicast) 6. Wsparcie dla IGMPv3 oraz MSDP 7. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych 8. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) 9. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) 10. Minimum 1000 wejściowych oraz min. 1000 wyjściowych wpisów dla ACL - access control list |  |
| Wsparcie mechanizmów bezpieczeństwa w sieci: | 1. Wsparcie ACL 2. Snooping 3. ARP Inspection |  |
| Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika: | 1. Port zarządzający 100/1000 Mbps; 2. Port konsoli CLI; 3. Ping 4. Traceroute. |  |
| Akcesoria: | 1. 2 szt. wkładek QSFP-100G-LR4-S 2. 2 szt. patchcord LCLC-SM-50CM 3. 15 szt. składek SFP-10G-SR 4. 6 szt. wkładek SFP+ SFP-25G-SR. |  |
| Zasilanie | 1. 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. |  |
| Obudowa | 1. maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.   W wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia (jednak nie większy niż 2U). |  |
| Gwarancja: | 1. min. 60 miesięcy 2. Gwarancja obejmuje wszystkie części składowe urządzenia. |  |
| Serwis | 1. Świadczony na miejscu u Zamawiającego 2. Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu. 3. Czas reakcji na zgłoszenie awarii max. do 60 min. 4. Wymagany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii. 5. Uszkodzone nośniki danych pozostają u Zamawiającego. 6. Kontakt z pracownikami serwisu będzie prowadzony w języku polskim. |  |

**8. Dostawa i wdrożenie zarządzalnych przełączników sieciowych do utworzenia rdzenia sieci LAN – 6 szt.**

Minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **Przedmiot zamówienia** | **Opis przedmiotu zamówienia/ parametry wymagane** | **Parametr oferowany** |
|  | Typ i liczba portów | 48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP |  |
|  | Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek: | * Gigabit Ethernet 1000Base-SX, * Gigabit Ethernet 1000Base-LX/LH, * 10Gigabit Ethernet 10GBase-SR, * 10Gigabit Ethernet 10GBase-LR, * • 10Gigabit Ethernet typu twinax (SFP+ - SFP+) |  |
|  | Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) | do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi, |  |
|  | Zasilanie i chłodzenie | * Urządzenie wyposażone jest w wbudowany zasilacz AC230V |  |
| Parametry wydajnościowe | | | |
|  | Przepustowość przełącznika (switching bandwidth) | min. 176 Gb/s (full duplex), |  |
|  | Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3 | min. 77.38 Mpps |  |
|  | Pamięć DRAM | Min. 512 MB |  |
|  | Pamięć flash | 256 MB |  |
|  | Wielkość bufora pakietów | 1.5 MB |  |
|  | Obsługa | * 256 aktywnych sieci VLAN * 15000 adresów MAC * 16 statycznych tras IPv4 * 16 statycznych tras IPv6 * 64 interfejsów SVI L3 * Obsługa MTU-L3 9198B * Obsługa ramek Ethernet Jumbo 10240B * 1024 grupy IGMP * 6 połączeń zagregowanych typu „port channel” * 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP * Ilość wpisów w listach kontroli dostępu Security ACL – 600 * • ilość wpisów w listach kontroli dostępu QoS ACL – 600 |  |
|  | Porty dostępowe przełącznika posiadają zgodność ze standardem | standard IEEE 802.3az EEE (Energy Efficient Ethernet) |  |
|  | Obsługa protokołu | NTP, LLDP i LLDP-MED |  |
|  | Obsługa | IGMPv1/2/3 i MLDv1/2 Snooping |  |
|  | Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC | Tak |  |
|  | Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad | Tak |  |
|  | Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego | Tak |  |
|  | Możliwość uruchomienia funkcji serwera DHCP | Tak |  |
|  | Mechanizmy związane z bezpieczeństwem sieci: | * Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level), * Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, * Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, * Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, * Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, * Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, * Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication), * Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, * Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), * Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, * Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, * Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP), * Funkcja Private VLAN, |  |
|  | Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: | * sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia, * bezpieczna sekwencja uruchamiania, * sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia. |  |
|  | Mechanizmy związane z zapewnieniem jakości usług w sieci: | * Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, * Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, * Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), * Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, * Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń, * Kontrola sztormów dla ruchu broadcast/multicast/unicast, * Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; |  |
|  | Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6 | Tak |  |
|  | Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących, | Tak |  |
|  | Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.), | Tak |  |
|  | Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow, | Tak |  |
| Zarządzanie | | | |
|  | Port konsoli, | Tak |  |
|  | Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika, | Tak |  |
|  | Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, | Tak |  |
|  | Obsługa protokołów | SNMPv3, SSHv2, https, syslog, |  |
|  | Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia | Tak/podać |  |
|  | Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki; | Tak/podać |  |
|  | Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU | Tak/podać |  |
|  | Akcesoria | * + - 1. 5 szt. wkładek SFP-10G-SR       2. 5 szt. Patchord LCLC-MM-OM3-50CM |  |
| Warunki Gwarancji i serwisu | | | |
|  | Gwarancja dla wszystkich urządzeń należących do przedmiotu zamówienia min 12 m-ce liczone od dnia podpisania protokołu odbioru | |  |
|  | Gwarancja obejmuje wszystkie części składowe urządzenia. | |  |
|  | Gwarantowany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii. | |  |
|  | Świadczony na miejscu u Zamawiającego | |  |
|  | Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu. | |  |
|  | Czas reakcji na zgłoszenie max. 60 min, rozpoczęcie naprawy w ciągu 24 godz. od zgłoszenia. | |  |
|  | Kontakt z pracownikami serwisu będzie prowadzony w języku polskim. | |  |

1. **Dostawa, instalacja oraz podłączenie zasilacza awaryjnego UPS z kartą SNMP**

Minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **Przedmiot zamówienia** | **Opis przedmiotu zamówienia/ parametry wymagane** | **Parametry oferowane (podać)** |
|  | Moc | min. 3000VA/2700W |  |
|  | Obudowa | Możliwość montażu na stojąco jak i w szafie rack 19” |  |
|  | Faza | 1 faza z uziemieniem |  |
|  | Typ baterii | 12V/9AH |  |
|  | Ilość baterii | min. 4 |  |
|  | Czas ładowania | max. 4 godzin regeneracji do 90% pojemności |  |
|  | Wejście |  |  |
|  | Napięcie  Zakres napięcia  Zakres częstotliwości | 208/220/230/240 VAC  110-300 VAC ± 5% przy 50% obciążenia  160-300 VAC ± 5% przy 100% obciążenia  40/70 Hz (automatyczne wykrywanie) |  |
|  | Wyjście |  |  |
|  | Napięcie wyjściowe  Regulacja napięcia AC (tryb baterii)  Zakres częstotliwości (tryb baterii)  Max czas przełączenia UPS w tryb zasilania akumulatorowego  Kształt fali (tryb baterii) | 208/220/230/240 VAC  ±1%  57~63 Hz lub 50 Hz ± 0.1 Hz  max. 4 ms  Czysta fala sinusoidalna |  |
|  | Możliwość wymiany baterii podczas pracy | Tak |  |
|  | Zabezpieczenie przed przeciążeniem, rozładowaniem i przeładowaniem | Tak |  |
|  | Wskaźniki |  |  |
|  | Wyświetlacz LCD | Poziom obciążenia, poziom naładowania akumulatora, tryb AC, tryb akumulatora, tryb obejścia i wskaźnik usterki |  |
|  | Alarm: |  |  |
|  | Tryb baterii | Dźwięk co 4 s |  |
|  | Niski poziom naładowania baterii | Dźwięk co 1 s |  |
|  | Przeciążenie | Dźwięk dwa razy na sekundę |  |
|  | Usterka | Ciągły sygnał dźwiękowy |  |
|  | Środowisko |  |  |
|  | Działanie w warunkach wilgotności | 20-90% wilgotności względnej przy 0-40°C (bez kondensacji) |  |
|  | Poziom hałasu | Mniej niż 50 dBA w odległości 1 metra |  |
|  | Czas podtrzymania w zależności od obciążenia | min. 11,5 min przy 50% obciążeniu bez dodatkowych akumulatorów |  |
|  | Wbudowany stabilizator AVR | Tak |  |
|  | Automatyczny restart podczas przywracania napięcia AC | Tak |  |
|  | Funkcja zimnego startu | Tak |  |
|  | Ładowanie w trybie wyłączenia | Tak |  |
|  | Wbudowany port komunikacyjny | USB, RJ, SNMP |  |
|  | Karta SNMP | Tak |  |
|  | Złącze wejście AC  Złącze wyjścia AC | min. 1x IEC 320 x14  min. 1x IEC 320 C19  min. 6x IEC 320 C13 |  |
|  | Zarządzanie |  |  |
|  | Interfejs RS 232/USB | Wsparcie Windows 2000/2003/XP/Vista/2008, Windows 7,8,10 Linux i MAC |  |
|  | Warunki Gwarancji i serwisu | |  |
|  | Gwarancja dla wszystkich urządzeń należących do przedmiotu zamówienia 24 m-ce liczone od dnia podpisania protokołu odbioru | Tak/podać |  |
|  | Gwarancja obejmuje wszystkie części składowe urządzenia. | Tak/podać |  |
|  | Gwarantowany czas naprawy awarii 24 godziny od momentu zgłoszenia. W przypadku niemożliwego usunięcia awarii w przeciągu 24 godz. Wykonawca jest zobowiązany dostarczyć urządzenie zamienne, o parametrach nie gorszych, na czas usunięcia awarii. | Tak/podać |  |
|  | Świadczony na miejscu u Zamawiającego | Tak/podać |  |
|  | Opieka serwisowa 24 godziny na dobę 7 dni w tygodniu. | Tak/podać |  |
|  | Czas reakcji na zgłoszenie max. 60 min, rozpoczęcie naprawy w ciągu 24 godz. od zgłoszenia. | Tak/podać |  |
|  | Kontakt z pracownikami serwisu będzie prowadzony w języku polskim. | Tak/podać |  |

1. **Dostawa wraz z montażem i uruchomieniem dysków 12TB przeznaczonych do wykonywania kopii zapasowych – 5 szt.**

Minimalne parametry techniczne:

|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **Przedmiot zamówienia** | **Minimalne parametry wymagane** | **Parametr oferowany** |
| 1 | Pojemność | 12 TB |  |
| 2 | Interfejs | SATA III (6 Gb/s) |  |
| 3 | Rozmiar | 3,5’’ |  |
| 4 | Prędkość obrotowa | 7200 RPM |  |
| 5 | Pamięć cache | 256 MB |  |
| 6 | Kompatybilność | Kompatybilność z systemami NAS, RAID, systemami przechowywania danych o wysokiej wydajności |  |
| 7 | Gwarancja | 36 miesięcy gwarancji |  |

…………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

**Załącznik 2 b**

**Wykaz oferowanego oprogramowania wraz z szczegółowym opisem technicznym**

**Cz. II - dostawa oprogramowania do monitorowania infrastrukturą sieci informatycznej i urządzeń dla jednostki podległej oraz dostawa usług chmurowych w ramach zabezpieczenia poczty i stron internetowych Gminy.**

**UWAGA!**

Zamawiający wymaga dołączenia wykazu oferowanego sprzętu do formularza ofertowego. W pozycji parametry oferowane należy umieścić opis techniczny umożliwiający Zamawiającemu jednoznaczne określenie szczególnych cech produktu oraz wymagane prawem certyfikaty, deklaracje zgodności CE, instrukcje obsługi sprzętu, dokumenty gwarancyjne, celem sprawdzenia zgodności oferowanego produktu.

**W przypadku nie dołączenia wymienionego powyżej wykazu do formularza oferty oferta podlega odrzuceniu jako niezgodna z zapisami swz.**

1. **Oprogramowanie do zarządzania infrastrukturą IT na 31 licencji**

Zamawiający wymaga dostarczenia oprogramowania wraz z licencjami spełniającego poniższe graniczne minimalne parametry techniczne.

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Przedmiot zamówienia** | **Minimalne parametry wymagane** | **Parametr oferowany** |
| 1. | Oprogramowanie: | 1. Budowa modułowa, 2. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. 3. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolę zarządzającą. 4. Silnik bazy danych musi być dostępny na licencji open source bez limitu ilości danych 5. Baza danych musi być darmowa i nie wymagać dodatkowego licencjonowania |  |
| 2. | Monitorowanie danych użytkownika: | 1. historia aktywności 2. polityka korzystania z Internetu i aplikacji 3. dostęp do zewnętrznych nośników danych, 4. grupowanie informacji w oddzielnym oknie, co umożliwia usuwanie danych użytkownika zgodne z RODO bez konieczności usunięcia informacji o stacji roboczej, 5. dostęp do danych osobowych oraz danych z monitoringu zgodnie z RODO, 6. możliwość nadawania kontom różnych poziomów dostępu oraz uprawnień do funkcji Programu, grup urządzeń i użytkowników, 7. lista kont użytkowników i administratorów, może być synchronizowana z usługą typu Active Directory, przez szyfrowane połączenia, 8. konfiguracja haseł użytkownika 9. uwierzytelnianie logowań do konsoli z wykorzystaniem weryfikacji dwuskładnikowej |  |
| 3. | Funkcjonalności: | Oprogramowanie obsługuje min. 6 funkcjonalności:   1. Monitorowanie infrastruktury, 2. Inwentaryzacja sprzętu i oprogramowania, 3. Monitorowanie aktywności użytkowników, 4. Realizacja zdalnej pomocy użytkownikom, 5. Ochrona danych przed wyciekiem, 6. Wsparcie zarządzania czasem i analizowanie aktywności użytkowników |  |
| 4. | Monitorowanie infrastruktury: | 1. Wykrywanie urządzeń w sieci poprzez skanowanie ping oraz arp-ping, 2. Wizualizacja urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki, tworzenie spersonalizowanych map z możliwością zablokowania mapy urządzeń przed przypadkową edycją, 3. Serwisy TCP/IP, HTTP, POP3, SMTP, FTP i inne wraz z możliwością definiowania własnych serwisów. Monitorowanie czasu ich odpowiedzi i procent utraconych pakietów, 4. Serwery pocztowe:  * program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty, * program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie, * program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa  1. Monitorowanie serwerów WWW i adresów URL 2. Cykliczne monitorowanie czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS 3. Obsługa szyfrowania SSL/TLS w powiadomieniach e-mail 4. Obsługa urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID 5. Obsługa komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych 6. Monitoringu routerów i przełączników wg:  * zmian stanu interfejsów sieciowych * ruchu sieciowego * podłączonych stacji roboczych – graficzna prezentacja panelu switcha * ruchu generowanego przez podłączone do portów stacje robocze  1. Monitor serwisów alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie, zatrzymanie lub zrestartowanie, 2. Wyświetlanie statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu 3. Monitorowanie stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano 4. Zarządzanie stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny 5. Wydajność systemów m.in. obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy, 6. Nakładanie na urządzenia liczników wydajności WMI oraz SNMP z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi, wyłączenie/restart komputera. 7. Administrator samodzielnie może konfigurować zdarzenia, lub wybrać zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. 8. Alarmy muszą pozwalać na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. 9. Oprogramowanie musi umożliwiać wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0 |  |
| 5. | Inwentaryzacja sprzętu i oprogramowania, | 1. Automatyczne gromadzenie informacji o sprzęcie i oprogramowaniu na stacjach roboczych, min. modelu, procesora, pamięci, płyty głównej, napędów, 2. Umożliwienie odczytów parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informacja o zainstalowanych aplikacjach oraz aktualizacjach systemu 5. Zbieranie informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Możliwość wysyłania powiadomienia np. e-mailem w przypadku jakiejkolwiek zmiany na urządzeniu 7. Możliwość odczytania numeru seryjnego (klucze licencyjne). 8. Możliwość automatycznego zarządzania instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Możliwość przeglądania informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Możliwość utworzenia listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Możliwość wymiany plików do i ze stacją roboczą poprzez funkcję Menedżera plików.   *Moduł inwentaryzacji zasobów musi umożliwiać prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:*   1. przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, 2. przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, 3. tworzenia powiązań między zasobami a urządzeniami, 4. tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z funkcjonującą w Urzędzie Active Directory ), wskazywanie osób odpowiedzialnych, 5. wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, 6. definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości, 7. określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, 8. określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, 9. masową edycję atrybutów zasobów, 10. definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, 11. importu danych z zewnętrznego źródła (.CSV), 12. przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., 13. tworzenia powiązań między zasobami a dokumentami w relacji 1:N, 14. oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., 15. ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, 16. generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, 17. przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, 18. konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, 19. konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, 20. archiwizacji i porównywania audytów zasobów, 21. tworzenia kodów kreskowych dla zasobów, 22. drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, 23. inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, 24. możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, 25. inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), 26. definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   *Inwentaryzacja oprogramowania musi zapewniać funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:*   1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji. 4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji, 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. |  |
| 6. | Monitorowanie aktywności użytkowników: | 1. Faktyczny czas aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), 2. Otwarte procesy wraz z informacją o uruchomieniu na podwyższonych uprawnieniach, 3. Rzeczywiste użytkowanie programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, 4. Informacja o edytowanych przez użytkownika dokumentach, 5. Historia pracy (cykliczne zrzuty ekranowe), 6. Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), 7. Transfer sieciowy użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), 8. Wydruki m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program powinien mieć możliwość monitorowania kosztów wydruków, 9. Nagłówki przesyłanej w aplikacjach klienckich poczty e-mail. 10. Wykrywanie podejrzanej aktywności przez popularne „jigglery”, mającej na celu symulowanie faktycznej pracy. 11. Zdefiniowanie czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. 12. Wyszczególnienie podejrzanej aktywności w raportach. 13. Wygenerowanie alarmu i wykonanie akcji po wykryciu podejrzanej aktywności. 14. Automatyczne włączenie zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. 15. Blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. \*.domena.pl). 16. Blokowania ruchu na wskazanych portach TCP/IP, 17. Blokowanie pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, 18. Prowadzenie rejestru naruszeń blokad, 19. Wysyłanie powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domeny; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, 20. Przygotowanie zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), 21. Definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. |  |
| 7. | Realizacja zdalnej pomocy użytkownikom | 1. Dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połącznie i opcją odrzucenia takiego połącznia przez użytkownika, 2. Możliwość równoczesnego podłączenia do tego samego komputera kilku administratorów. 3. Oprogramowanie powinno zawierać komunikator (czat), który umożliwi prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów.   Czat powinien pozwalać na:   1. zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej 2. rozmowy między „zwykłymi” użytkownikami 3. przesyłanie plików między rozmówcami w trybie online 4. tworzenie pokojów tematycznych, rozmów grupowych 5. oznaczanie kontaktów jako „ulubionych” na liście kontaktów 6. uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku, 7. Administrator powinien mieć możliwość tworzenia szkiców i archiwizowania komunikatów.   Moduł pomocy zdalnej powinien umożliwiać:   1. pobieranie listy użytkowników z Active Directory, 2. wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, 3. zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, 4. zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez system zarządzania regułami widoczności zgłoszeń, 5. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, 6. zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, 7. tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, 8. automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, 9. definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, 10. przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, 11. procesowanie zgłoszeń użytkowników z wiadomości e-mail, 12. eksportowania listy zgłoszeń do plików CSV i XLSX, 13. integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, 14. tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, 15. wykonywanie operacji na wielu zgłoszeniach równocześnie, 16. dołączanie załączników do zgłoszeń, 17. rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, 18. szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, 19. wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, 20. zrzuty ekranowe (podgląd pulpitu), 21. zdalną modyfikację rejestrów, 22. dystrybucję oprogramowania przez Agenty, 23. dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), 24. możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, 25. możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, 26. planowanie nieobecności pracowników helpdesk, 27. obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, 28. generowanie raportów obsługi helpdesk, 29. zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), 30. zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), 31. wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików. |  |
| 8. | Ochrona danych przed wyciekiem | Blokowanie urządzeń i nośników danych:   1. możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. 2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. 3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. 4. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezaufanych. 5. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender. 6. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker. 7. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker. 8. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu. 9. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu. 10. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender 11. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.   Zarządzanie prawami dostępu do urządzeń:   1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. 2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive’ów, dysków itp. 3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników. 4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci. 5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.   Audyt operacji na plikach na urządzeniach przenośnych:   1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 2. Podłączenie/odłączenie urządzenia przenośnego. 3. Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika. 4. Definiowanie reguł monitorowanych folderów w postaci list. Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agenta (np. macierze, NAS itp.) Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. |  |
| 9. | Zarządzanie czasem i analizowanie aktywności użytkowników | 1. Możliwość oznaczenia sesji aktywności jako czas prywatny gdy pracownik wykonuje czynności prywatne na sprzęcie firmowym. 2. Użytkownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. 3. Zastosowane reguły powinny pozwalać zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. 4. Dostęp powinien być realizowany przez przeglądarkę internetową, a strona powinna być wyświetlana w trybie jasnym lub ciemnym. 5. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 6. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 7. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 8. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 9. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 10. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 11. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 12. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 13. Wskaźnik czasu poświęconego na aktywność produktywną. 14. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 15. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 16. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów. |  |
| 10. | Gwarancja, wsparcie serwisowe | 1. Wsparcie techniczne przez min. rok od dnia podpisania protokołu odbioru 2. W ramach wsparcia technicznego możliwość instalowania wszelkich aktualizacji oprogramowania, które zostaną wydane w czasie obowiązywania wsparcia, w tym aktualizacji obejmujących przejście na wyższą wersję oprogramowania. 3. Telefoniczne i mailowe wsparcie techniczne dla oprogramowania 4. Dokonywanie przez Producenta szczegółowej analizy zgłoszonych przypadków (logów). 5. Świadczenie przez Producenta pomocy w formie sesji zdalnych. 6. Czas reakcji na zgłoszenie nie dłuższy niż następny dzień roboczy. 7. Możliwość przedłużenia wsparcia o kolejny rok 8. Możliwość rozszerzenia oprogramowania o dodatkowe licencje i moduły |  |

1. **Usługa zabezpieczenia poczty na 24 miesiące**
   * + 1. Zamawiający w ramach przedmiotu zamówienia wymaga dostarczenia usługi zabezpieczenia poczty spełniającej poniższe minimalne parametry techniczne:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Minimalne parametry wymagane** | | | **Parametr oferowany** | |
|  | system ochrony poczty elektronicznej przed wiadomościami niepożądanymi typu spam, wirusy i oprogramowanie złośliwe, phishing, wyłudzenia, podszywanie, manipulacja tożsamością i inne zagrożenia bezpieczeństwa informatycznego. | | |  | |
|  | System filtrujący, portal konfiguracji polityki bezpieczeństwa, system zarządzania i raportowania dostępne jako usługi chmurowe | | |  | |
|  | ochrona przed wiadomościami niepożądanymi za pomocą filtracji poczty przychodzącej i ochronę reputacji własnego systemu pocztowego przez filtrację poczty wychodzącej. | | |  | |
|  | Przekierowanie ruchu pocztowego do chmury obsługiwane na poziomie konfiguracji rekordów Mail Exchange (MX) w systemie DNS. | | |  | |
|  | Chmurowy system ochrony powinien umożliwiać obsługę wielu domen pocztowych jednocześnie (nie mniej niż 15). | | |  | |
|  | Chmurowy system ochrony powinien zapewniać ochronę przed wolumetrycznymi atakami Denial-of-Service | | |  | |
| **Funkcjonalność filtracji poczty przychodzącej:** | | | | | |
|  | Filtracja wiadomości typu spam: | | * wszystkie przychodzące wiadomości powinny być klasyfikowane pod kątem prawdopodobieństwa, że jest to wiadomość typu spam * klasyfikacja powinna być automatyczna i pracować bez ingerencji administratora lub konfiguracji * możliwość zaprogramowania poziomu tolerancji na spam: od całkowitej blokady do całkowitej akceptacji wszystkich wiadomości sklasyfikowanych jako spam * możliwość zaprogramowania typu reakcji na spam: co najmniej „blokada”, „kwarantanna”, „akceptacja”, |  | |
|  | | Filtracja wiadomości ze względu na kategorię komunikacji: | * oprócz filtrowania wiadomości typu spam system powinien rozpoznawać inne, często niejednoznaczne kategorie komunikacji, co najmniej: komunikację służbową, komunikację handlową, komunikację marketingową, komunikację związaną z listami mailingowymi, komunikację związaną z mediami społecznościowymi, komunikację rozsyłaną masowo * dla każdej rozpoznanej kategorii powinna być możliwość zaprogramowania reakcji, co najmniej: „blokada”, „kwarantanna”, „akceptacja” | |  | |
|  | | Filtracja wiadomości zawierających wirusy i oprogramowanie złośliwe, zagrożenia ATP i zagrożenia Zero-Day | * możliwość skanowania przez silnik antywirusowy * możliwość skanowania przez silnik sandboxingowy: wykrywanie zagrożeń zamaskowanych typu *Advanced Persistent Threats* (ATP) i zagrożeń typu *Zero-Day* * polityka skanowania ATP powinna umożliwiać konfigurację wyjątków opartych na adresach IP, na adresach nadawców i odbiorców poczty elektronicznej | |  | |
|  | | Filtracja wiadomości phishingowych, wiadomości związanych z wyłudzeniami, ochrona przed złośliwymi adresami URL: | * możliwość filtrowania wiadomości pod kontem phishingu, inżynierii socjalnej, próbami wyłudzeń i kradzieży tożsamości * możliwość filtrowania i ochrony adresów URL zawartych w wiadomościach przed złośliwym wykorzystaniem i zmianą zawartości po dostarczeniu do odbiorcy (*link protection, typosquatting protection* | |  | |
|  | | Filtracja wiadomości na podstawie informacji geograficznych (GeoIP) i językowych | * możliwość blokowania lub umieszczania w kwarantannie poczty przychodzącej z wybranego kraju (np. z Somalii) * możliwość blokowania lub umieszczania w kwarantannie poczty w określonym języku (np. chińskim) | |  | |
|  | | Filtracja wiadomości na podstawie zawartości - możliwość blokowania lub umieszczania w kwarantannie | * wiadomości z załącznikami o określonej nazwie lub o okroślonym typie MIME * wiadomości z załącznikami zaszyfrowanymi, co najmniej: archiwa takie jak ZIP, pliki Microsoft Office, pliki PDF * wiadomości zawierających wskazane słowa kluczowe w nagłowkach, temacie, zawartości lub w załącznikach | |  | |
|  | | Filtracja wiadomości przychodzących na podstawie polityk DNS, SPF, DKIM i DMARC | * możliwość weryfikacji domeny nadawcy: blokowanie nadawców z nieskonfigurowanym rekordem PTR * możliwość weryfikacji nadawcy za pomocą polityki *Sender Policy Framework (SPF)* * możliwość weryfikacji nadawcy za pomocą polityki *Domain Key Identified Email (DKIM)* * możliwość weryfikacji nadawcy za pomocą polityki *Domain Based Message Authentication (DMARC)* | |  | |
| *Funkcjonalność związana z kwarantanną i buforowaniem wiadomości:* | | | | | |
|  | Kwarantanna i buforowanie wiadomości | | * możliwość pracy z kwarantanną indywidualną, skonfigurowaną i dostępną per użytkownik * możliwość pracy z kwarantanną globalną |  | |
|  | Buforowanie i udostępnianie wiadomości w przypadku awarii docelowego serwera pocztowego: | | * odbiór i buforowanie wiadomości przychodzących do czasu usunięcia awarii docelowego serwera pocztowego (co najmniej 96 godzin) * udostępnienie zbuforowanych wiadomości użytkownikom za pomocą interfejsu webowego, pozwalającego odczytywać i odpowiadać na wiadomości w czasie awarii * synchronizację wiadomości z serwerem docelowym po usunięciu awarii |  | |
|  | Buforowanie wiadomości przychodzących | | * system powinien umożliwiać administratorowi przeszukiwanie przychodzących transmisji, co najmniej z ostatnich 30 dni * system powinien umożliwiać zmianę decyzji blokującej wiadomość z ostatnich 30 dni i dostarczenie zablokowanej wiadomości do odbiorcy |  | |
| **Funkcjonalność filtracji poczty wychodzącej:** | | | | | |
|  | skanowanie wiadomości wychodzących: | | * wiadomości zawierające wirusy powinny być blokowane * wiadomości podejrzane o spam powinny być blokowane lub poddane kwarantanni |  | |
|  | Filtracja wiadomości wychodzących z możliwością kwarantanny: | | * filtracja nazw i typów MIME załączonych plików * filtracja zaszyfrowanych i chronionych hasłem plików archiwów, plików Microsoft Office, plików PDF * filtracja na podstawie słów kluczowych w nagłowkach, temacie, zawartości, załącznikach, adresie nadawcy lub adresie odbiorcy |  | |
| **Monitorowanie i raportowanie:** | | | | | |
|  | Możliwość wyświetlania raportów i eksportu raportowanych danych do pliku, co najmniej | | * analiza ruchu pocztowego przychodzącego i wychodzącego w zadanym czasie: liczba wiadomości przychodzących, zablokowanych, zablokowanych ze względu na spam, wirusy lub zagrożenia ATP * analiza użytkowników: odbiorcy i nadawcy spamu i wirusów   analiza użytkowników: najczęściej blokowani odbiorcy i nadawcy |  | |
| **Funkcjonalność związana z integracją z systemami zewnętrznymi** | | | | | |
|  | Możliwość integracji z zewnętrznym systemem monitorowania | | * wsparcie dla protokołu SYSLOG z szyfrowaniem w standardzie TLS |  | |
| Warunki Gwarancji i serwisu | | | | | |
|  | Wsparcie techniczne musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego producenta z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu | | |  | |
|  | Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 15:00 (e-mail; telefon) 24x7 poprzez zgłoszenie Email. | | |  | |

1. **Usługa zabezpieczenia serwisu www na 24 miesiące:**

Zamawiający w ramach przedmiotu zamówienia wymaga dostarczenia do Zamawiającego usługi zabezpieczenia serwisu stron internetowych na 24 miesiące spełniającego minimalne parametry techniczne opisane poniżej:

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis przedmiotu zamówienia/ Minimalne parametry wymagane** | **Parametr oferowany** |
|  | Dostęp do platformy umożliwiającej ochronę wybranych stron internetowych. |  |
|  | Dostarczona usługa w postaci subskrypcji ważnej 24 miesiące powinna:  posiadać funkcje ochrony Web Application Firewall (WAF) i Captcha,  - zapewniać zaawansowaną ochronę przed atakami DDoS,  - umożliwiać dostęp do globalnej sieć dostarczania treści (CDN),  - zapewniać szyfrowanie i optymalizację SSL,  - obsługiwać IPv6,  - automatycznie buforować treści statyczne,  - zapewnić utrzymanie statycznych elementów serwisu online również w przypadku awarii serwera,  - zapewnić zabezpieczenie przed kopiowaniem treści, w tym tekstu, obrazów i adresów e-mail przed mechanizmami automatycznie zbierającymi treści z Internetu,  - uniemożliwiać dostępu do serwisu z indywidualnych adresów IP, zakresów adresów, lub z określonych krajów. |  |
|  | poprawa wydajności strony internetowej |  |
|  | działa jako autorytatywny serwer DNS, co odpowiada za kierowanie ruchu do strony internetowej. |  |
|  | możliwość samodzielnego zarządzania usługą poprzez panel administracyjny, możliwość skalowania i elastycznego dobierania funkcjonalności, |  |
|  | zapewnienie regionalnego (PL) podstawowego wsparcia technicznego w minimalnym przedziale od poniedziałku do piątku w godzinach min. 08:00 – 15:00. |  |

…………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

Załącznik nr 3

**Oświadczenie Wykonawcy**

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych

**o niepodleganiu wykluczeniu**

z uwzględnieniem przesłanek na podstawie art.7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z postępowania o udzielenie zamówienia pn.: ***,,Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***

**Gmina Miastko**

**ul. Grunwaldzka 1**

**77-200 Miastko**

**Wykonawca:**

..................................................................................................................................................................................................

..................................................................................................................................................................................................

*(pełna nazwa)*

reprezentowany przez …………………………………………………………………………………………………………....

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

Adres/siedziba…..…………………………………………………………………………………………………………

NIP……………………………………………………………………………………………………………………

REGON…………………………………………………………………………………………………………………

*(w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich członków konsorcjum)*

Na potrzeby niniejszego postępowania, oświadczam, co następuje:

**1. Oświadczenie dotyczące wykonawcy**

1) **Oświadczam**, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Pzp.

…………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

2) **Oświadczam**, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. 108 ust. 1 w związku z przesłankami określonymi w ust. 1 pkt……………..przywołanego artykułu.

*(wskazać pkt w art. 108 ust. 1 Pzp - przypisany do przesłanki lub przesłanek, które wystąpiły)*

Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. Art. 110 ust. 2 Pzp podjąłem następujące środki naprawcze:

……………………………………………………………………………………………………………

…………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

**2. Oświadczam,** że nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

…………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

*( Podpisać właściwe oświadczenie wskazane w pkt 1 –3, pozostałe wykreślić)*

**3. Oświadczenie dotyczące podanych informacji**

**Oświadczam,** że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

………………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

Załącznik nr 4

**Oświadczenie wykonawcy**

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych **o spełnianiu warunków udziału** w postępowaniu o udzielenie zamówienia pn.: ***,,Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***

**Gmina Miastko**

**ul. Grunwaldzka 1**

**77-200 Miastko**

**Wykonawca:**

..................................................................................................................................................................................................................................................................................................................................................................  *(pełna nazwa)*

reprezentowany przez …………………………………………………………………………………………………………....

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

Adres/siedziba……………………………………………………………………………………………………………

NIP………………………………………………………………………………………………………………………

REGON……………………………………………………………………………………………………………………

*(w przypadku składania oferty przez podmioty występujące wspólnie podać nazwy (firmy) i dokładne adresy wszystkich członków konsorcjum)*

Na potrzeby niniejszego postępowania, oświadczam, co następuje:

* + 1. **Informacja dotycząca wykonawcy**

**Oświadczam**, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Rozdziale …………… Specyfikacji Warunków Zamówienia.

* + 1. **Informacja w związku z poleganiem na zasobach innych podmiotów**

**Oświadczam**, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w Rozdziale … Specyfikacji Warunków Zamówienia*,* polegam na zasobach następującego/ych podmiotu/ów:

1. ………………………………………………………………………...……………...…………………………………………………………………………….………………………………….…………………  
   w następującym zakresie: …………………………………………………………………………………….

*(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)*

1. ………………………………………………………………………...……………...………………………….……………………………………………….……………………………..…….……………………  
   w następującym zakresie: ……………………………………………………………………………….

*(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)*

1. ………………………………………………………………………...……………...………………………………………………………………………….…………….…………………………………………  
   w następującym zakresie: ……………………………………………………………………………….

*(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu)*

* + 1. **Oświadczenie dotyczące podanych informacji**

**Oświadczam,** że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

…………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

Załącznik nr 5

**Oświadczenie Wykonawcy**

o braku przynależności do tej samej grupy kapitałowej, w zakresie art. 108 ust. 1 pkt 5 Pzp, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2024 r. poz. 594 z późn. zm.) w postępowaniu o udzielenie zamówienia pn.: ***,,Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***

**Gmina Miastko**

**ul. Grunwaldzka 1**

**77-200 Miastko**

**Wykonawca:**

.........................................................................................................................................................................................................................................................................................................................................................….....  *(pełna nazwa wykonawcy)*

reprezentowany przez …………….………………………………………………………………………………....

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

Adres………………………………………………………………………………………………………

NIP………………………………………………………………………………………………………

REGON…………………………………………………………………………………………………………

*(w przypadku składania oferty przez Wykonawców występujących wspólnie – każdy z uczestników składa odrębne oświadczenie podając swoją nazwę (firmę) i  adres)*

W celu wykazania braku podstaw wykluczenia z postępowania na podstawie art. 108 ust. 1 pkt 5 Pzp,

**Oświadczam, że\* -** w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2024 r. poz. 594 z późn. zm.).**:**

 **nie należę** (nie należymy) do tej samej grupy kapitałowej,

 **należę** (należymy) do tej samej grupy kapitałowej:

………………………………………………………………………………………………………

………..……………………………………………………………………………………………..

*(wymienić podmioty wchodzące w skład tej samej grupy kapitałowej podając ich nazwę (firmę) i  adres)*

oraz składam wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.

\* zaznaczyć odpowiednie

…………….……. *(miejscowość),* dnia ………….……. r. …………………………………………

*(podpis wykonawcy lub osób uprawnionych*

*do występowania w jego imieniu )*

Załącznik nr 6

**Oświadczenie podmiotu/ów**

udostępniającego/ch zasoby, na których może polegać Wykonawca w zakresie zdolności technicznych   
lub zawodowych lub sytuacji finansowej lub ekonomicznej, w celu potwierdzenia spełniania warunków udziału w postępowaniu – składane na podstawie art. 125 ust. 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych,

**o braku podstaw wykluczenia oraz spełnianiu warunków udziału**

z uwzględnieniem przesłanek na podstawie art.7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego z postępowania o udzielenie zamówienia pn.:***,,Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***

**Gmina Miastko**

**ul. Grunwaldzka 1**

**77-200 Miastko**

**Nazwa Podmiotu:**

....................................................................................................................................................................................................................................................................................................................................................................................................  *(pełna nazwa)*

reprezentowany przez …………………………………………………………………………………………………………....

*(imię, nazwisko, stanowisko/podstawa do reprezentacji)*

Adres………………………………………………………………………………………………………………………

NIP…………………………………………………………………………………………………………………………

REGON………………………………………………………………………………………………………………

Na potrzeby niniejszego postępowania, **oświadczam, że:**

1. nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Pzp oraz spełniam warunki udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuję się na udostępnione przeze mnie zasoby:
2. nie zachodzą w stosunku do mnie przesłanki wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

.

……………*(miejscowość),* dnia ………….……. r. ……………………………………………………

*(podpis podmiotu udostępniającego zasoby lub osób uprawnionych do występowania w jego imieniu*

Załącznik nr 7

**Zobowiązanie Podmiotu**

udostępniającego zasoby, do oddania do dyspozycji Wykonawcy, niezbędnych zasobów na potrzeby realizacji zamówienia - składane na podstawie art. 118 ust. 3 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, w postępowaniu o udzielenie zamówienia publicznego pn.: ***,,Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***

Ja/My niżej podpisani:

……………………………….....................................................................................................................

*(imię i nazwisko osoby/ób upoważnionej/ych do reprezentowania Podmiotu udostępniającego zasoby – zgodnie z zasadami reprezentacji Podmiotu składającego zobowiązanie)*

*, który występowania w jego imieniu )nazwa (podpis podmiotu udostępniającego zasoby lub osób uprawnionych do występowania w jego imieniu )nazwa (firma) i dokładny adres Podmiotu oddającego Wykonawcy do dyspozycji zasoby na zasadach określonych w art. 118 Pzp)*

działając w imieniu i na rzecz:

………………………………................................................................................................................................ *(nazwa (firma) i dokładny adres Podmiotu oddającego Wykonawcy do dyspozycji zasoby na zasadach określonych w art. 118 Pzp)*

zobowiązuję/my się oddać do dyspozycji uczestniczącemu w niniejszym postępowaniu Wykonawcy:

……………………………….................................................................................................................................

……………………………………………………………………………………………………………………*(nazwa (firma) i dokładny adres Wykonawcy, który polega na zasobach ww. podmiotu na zasadach określonych w art. 118 Pzp)*

następujące niezbędne zasoby na potrzeby realizacji ww. zamówienia:

…….…………………………...................................................................................................................…… *(określenie zasobu, np. wiedza i doświadczenie, potencjał techniczny, potencjał kadrowy, potencjał ekonomiczno-finansowy)*

Sposób wykorzystania udostępnionych przeze mnie zasobów będzie następujący:

……………………………….....................................................................…………............................................

Charakter stosunku łączącego mnie z Wykonawca będzie następujący:

……………………………….....................................................................................................................

Zakres mojego udziału przy wykonywaniu zamówienia będzie następujący:

……………………………….....................................................................................................................

……………*(miejscowość),* dnia ………….……. r. …………………...…………………………………………

*(podpis/y Podmiotu udostępniającego zasoby lub osoby/ób uprawnionych do występowania w jego imieniu )*

Załącznik nr 8

**Wykaz dostaw**

**wykonanych w okresie 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie wraz z podaniem ich przedmiotu, dat wykonania i podmiotów, na rzecz których wykonywane zostały dostawy oraz załączenie dowodów czy te dostawy zostały wykonane należycie.**

Na potrzeby postępowania o udzielenie zamówienia publicznego w trybie podstawowym na wykonanie zamówienia pn.**,, *Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***przedkładam niniejszy wykaz dostawwykonanych w okresie 3 lat przed upłynięciem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy- w tym okresie wraz z podaniem ich przedmiotu, dat wykonania i podmiotów, na rzecz których wykonywane zostały dostawy oraz załączenie dowodów czy te dostawy zostały wykonane należycie.

**UWAGA:** Wykonawca jest zobowiązany wypełnić wszystkie rubryki, podając kompletne i jednoznaczne informacje, z których wynikać będzie spełnienie warunku w opisanego w rozdziale XIV SWZ. Wskazana dostawa dotyczy jednego wykonanego kontraktu (wynika z jednostkowej umowy zawartej z danym podmiotem). Jeżeli w ofercie zostanie wskazana więcej niż jedna część zamówienia wówczas wartość dostaw nie może być niższa niż suma wymaganych wartości dostaw dla wszystkich części wskazanych w ofercie.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rodzaj dostaw | Wartość dostaw brutto | Daty wykonania  od – do | Miejsce wykonania | Podmiot na rzecz, którego dostawy te zostały wykonane |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Wraz z wykazem należy załączyć dokument/dowody potwierdzające, że wymienione w wykazie dostawy została lub jest wykonywana należycie.**

Dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy:

……………………………………………….

*Podpis wykonawcy lub osoby upoważnionej do występowania*

*w jego imieniu*

Załącznik nr 9

**Wykaz osób skierowanych do realizacji zamówienia**

w postępowaniu o udzielenie zamówienia publicznego o wartości mniejszej niż progi unijne określone w przepisach wydanych na podstawie art. 3 ust. 3 Pzp, prowadzonym w trybie podstawowym, o którym mowa w art. 275 pkt 1 Pzp pn.:***,, Dostawa i wdrożenie infrastruktury sprzętowej w ramach rozbudowy sieci informatycznej Gminy Miastko.”***

**Gmina Miastko**

**ul. Grunwaldzka 1**

**77-200 Miastko**

Składając ofertę w przedmiotowym postepowaniu oświadczam, że dysponuję osobą posiadającą doświadczenie zawodowe gwarantujące należyte wykonanie zamówienia w zakresie niezbędnym do wykazania spełnienia warunku - określonego w Rozdziale XIV swz:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Imię i nazwisko | Doświadczenie zawodowe w latach | Nazwa przeprowadzonej  usługi szkoleniowej/ zakres | Termin  przeprowadzonej  usługi  szkoleniowej | Podmiot, na rzecz którego usługi zostały wykonane (nazwa i adres) |
|  |  |  |  |  |
|  |  |  |  |  |

**Wraz z wykazem należy załączyć dokument/dowody potwierdzające, że wymienione w wykazie osoby posiadają odpowiednie kwalifikacje oraz ze usługi przeprowadzenia wystąpień/szkoleń/prelekcje związanych z tematyką bezpieczeństwa informacji wykonywana należycie.**

Dowodami, o których mowa są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi zostały wykonane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy

……………*(miejscowość),* dnia ………….……. r. …………………...…………………………………………

*(podpis/y Podmiotu udostępniającego zasoby lub osoby/ób uprawnionych do występowania w jego imieniu )*