Znak sprawy: A.ZO.1.23  **ZAŁĄCZNIK NR 1**

**Do zapytania ofertowego**

**………………………….**

**Miejscowość data**

**FORMULARZ CENOWO – OFERTOWY**

**Część I**

|  |  |
| --- | --- |
| **Nazwa Wykonawcy**  (pieczęć firmowa) |  |
| **Adres siedziby Wykonawcy** |  |
| **NIP Wykonawcy** |  |
| **Telefon do Wykonawcy** |  |
| **E-mail do Wykonawcy** |  |
| **Osoba do kontaktu**  (Imię i nazwisko oraz dane kontaktowe) |  |

***Odpowiadając na zapytanie ofertowe z dnia 28.04.2023 pn.:*** ***„Dostawa sprzętu komputerowego w ramach projektu grantowego „Cyfrowa Gmina” realizowanego w ramach POPC 2014-2020”, oferuję wykonać / dostarczyć przedmiot zamówienia, na warunkach określonymi poniżej:***

Zamawiający wymaga aby zaoferowany sprzęt/oprogramowanie posiadał parametry nie gorsze niż:

**CZĘŚĆ I**

A)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Szczegółowy opis** | | | | **Parametry oferowane** | | |
| Komputer stacjonarny typu all in one.  W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy (numer konfiguracji lub part numer) oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.   Jeśli na stronie internetowej producenta nie jest dostępna pełna oferta modeli sprzętu wraz z jego konfiguracją, do oferty należy dołączyć katalog producenta zaoferowanego produktu umożliwiający weryfikację oferty pod kątem zgodności z wymaganiami Zamawiającego.  Nie dopuszcza się zaoferowania komputera odnawianego. | | | | Producent: ……………………….  Model:  ……………………….  Numer katalogowy (numer konfiguracji lub part numer): ………………………. | | |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** | | | **Parametry** | | |
|  | Procesor | Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach min. 21 600 pkt. w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na http://www.cpubenchmark.net/.  Testy pochodzące z okresu od publikacji postępowania do dnia składania ofert.  Wydruk z wynikami testów należy załączyć do oferty. | | | Producent: ………………………………  Model: …………………………… | | |
|  | Pamięć operacyjna RAM | Min. 16 GB 4800MHz non-ECC | | | Ilość pamięci RAM: ………….. | | |
|  | Parametry pamięci masowej | M.2 512 GB SSD PCIe 4.0 NVMe  Możliwość montażu dodatkowego dysku 2,5” SSD lub HDD | | | Ilość pamięci masowej: ………….. | | |
|  | Karta graficzna | Zintegrowana z procesorem komputera o wydajności min. 2 600 punktów w teście Average G3D Mark. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu. Wynik testu musi pochodzić z okresu od publikacji postępowania do terminu jego składania. | | | Producent: ………………………………  Model: ……………………………… | | |
|  | Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.  Wbudowane w obudowie komputera: głośniki stereo (2x3W)  Port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO)  Kamera video z mechaniczną zasłoną obiektywu o rozdzielczości min. 5 MPix i wsparciem dla Windows Hello  Dwa mikrofony wbudowane w obudowę komputera | | | Spełnia / Nie spełnia | | |
|  | Obudowa | * Zintegrowana z monitorem (AIO) * Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym * Możliwość podpięcia linki zabezpieczającej przez zintegrowane z obudową złącze np. Kensington Lock, Noble Lock | | | Spełnia / Nie spełnia | | |
|  | Płyta główna | Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. | | | Spełnia / Nie spełnia | | |
|  | Zgodność z systemami operacyjnymi | Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera ). | | | Spełnia / Nie spełnia | | |
|  | Bezpieczeństwo | TPM 2.0 | | | Spełnia / Nie spełnia | | |
|  | Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji). | | | Spełnia / Nie spełnia | | |
|  | BIOS | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera.  Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:  - wersji BIOS wraz z datą produkcji BIOS  - nr seryjnym komputera  - Ilości zainstalowanej pamięci RAM  - typie procesora i jego prędkości - MAC adresu zintegrowanej karty sieciowej  - nr seryjnym płyty głównej komputera  - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS    Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:   * Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS * Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. * Funkcja bezpiecznego usuwania danych z dysku | | | Spełnia / Nie spełnia | | |
|  | Ekran | Matowy, matryca IPS lub WVA, 23,8” z podświetleniem w technologii LED  Rozdzielczość FHD 1920x1080,  Jasność min. 250nits, kontrast 1000:1  Podstawa komputera umożliwiająca regulację wysokości (do 100mm) i pochylenia | | | Spełnia / Nie spełnia | | |
|  | Interfejsy / Komunikacja | Wyposażony w minimum:  3x USB typ C w tym min. 2 USB w standardzie 3.x  3x USB typ A w tym min. 2 USB w standardzie 3.x  1x RJ-45  1x HDMI out w standardzie min. 2.0  1x HDMI in w standardzie min. 1.4  1x port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO) | | | Spełnia / Nie spełnia | | |
|  | Karta sieciowa LAN | RJ-45 - 100/1000 | | | Spełnia / Nie spełnia | | |
|  | Karta sieciowa WLAN | Wbudowana karta sieciowa, pracująca w standardzie AX 2x2  Bluetooth 5.1 | | | Spełnia / Nie spełnia | | |
|  | Klawiatura i mysz | Klawiatura bezprzewodowa w układzie US. Mysz bezprzewodowa z rolką (scroll)  Klawiatura i mysz działające na jednym adapterze lub za pomocą połączenia bluetooth. | | | Spełnia / Nie spełnia | | |
|  | Zasilacz | Energooszczędny zasilacz o sprawności min. 85 % i mocy nie mniejszej niż 150W | | | Spełnia / Nie spełnia | | |
|  | Certyfikaty, oświadczenia i standardy | ENERGY STAR min. 8.0  EPEAT na poziomie min. Silver  Deklaracja zgodności CE  Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki  Certyfikat ISO 9001 dla producenta komputera  Certyfikat ISO 14001 dla producenta komputera  Certyfikat ISO 50001 dla producenta komputera | | | Spełnia / Nie spełnia | | |
|  | Waga/Wymiary | Waga urządzenia z podstawą nie może przekraczać 8 kg. | | | Spełnia / Nie spełnia | | |
|  | System operacyjny | Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:  1. Dostępne dwa rodzaje graficznego interfejsu użytkownika:  a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,  b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych  2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego  3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim  4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI.  5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe  6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,  7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików.  8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim  9. Wbudowany system pomocy w języku polskim.  10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).  11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.  12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer.  13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące.  14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.  15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.  16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".  17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.  18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.  19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.  20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.  21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.  22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.  23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."  24. Wbudowany mechanizm wirtualizacji typu hypervisor."  25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.  26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.  27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.  28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).  29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.  30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.  31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.  32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM  33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.  34. Możliwość tworzenia wirtualnych kart inteligentnych.  35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot)  36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.  37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.  38. Mechanizmy logowania w oparciu o:  a. Login i hasło,  b. Karty inteligentne i certyfikaty (smartcard),  c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),  d. Certyfikat/Klucz i PIN  e. Certyfikat/Klucz i uwierzytelnienie biometryczne  39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5  40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.  41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach  42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń  43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń | | | Producent: …………………..  Wersja: ………………….. | | |
|  | Oprogramowanie do aktualizacji sterowników | Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. | | | Spełnia / Nie spełnia | | |
|  | Gwarancja | Minimalny czas trwania gwarancji producenta wynosi 3 lata, świadczona w miejscu użytkowania sprzętu (on-site).  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.  W przypadku niewywiązywania się z obowiązku serwisowego przez Autoryzowanego Partnera Serwisowego lub Wykonawcę producent przejmie na siebie obowiązek serwisowy.  Komputery musza pochodzić z polskiej dystrybucji producenta.  Zamawiający może wystąpić do wykonawców o oświadczenie producenta komputera, potwierdzające spełnienie ww. warunków. | | | Spełnia / Nie spełnia | | |
|  | Wsparcie techniczne producenta | * Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera * Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. * Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera * Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00   Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie.  Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta.  Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta. | | | Spełnia / Nie spełnia | | |
| Wartość jednostkowa netto w zł | | | *Wpisać kwotę jednostkową* | | |
| Wartość jednostkowa brutto w zł | | | *Wpisać kwotę jednostkową* | | |

**B)**

|  |  |
| --- | --- |
| **Urządzenie UTM – 1 sztuka**  **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | **Wpisać nazwę lub model:** |

|  |  |
| --- | --- |
| Wymagania Ogólne |  |
| Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. |  |
| System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. | Spełnia / Nie spełnia |
| W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. | Spełnia / Nie spełnia |
| System musi wspierać IPv4 oraz IPv6 w zakresie: |  |
| * Firewall. | Spełnia / Nie spełnia |
| * Ochrony w warstwie aplikacji. | Spełnia / Nie spełnia |
| * Protokołów routingu dynamicznego. | Spełnia / Nie spełnia |
| Redundancja, monitoring i wykrywanie awarii |  |
| 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. | Spełnia / Nie spełnia |
| 1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. | Spełnia / Nie spełnia |
| 1. Monitoring stanu realizowanych połączeń VPN. | Spełnia / Nie spełnia |
| 1. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. | Spełnia / Nie spełnia |
| Interfejsy, Dysk, Zasilanie: |  |
| 1. System realizujący funkcję Firewall musi dysponować minimum: | Spełnia / Nie spełnia |
| * 10 portami Gigabit Ethernet RJ-45. | Spełnia / Nie spełnia |
| 1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. | Spełnia / Nie spełnia |
| 1. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. | Spełnia / Nie spełnia |
| 1. System musi być wyposażony w zasilanie AC. | Spełnia / Nie spełnia |
| Parametry wydajnościowe: |  |
| 1. W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. | Spełnia / Nie spełnia |
| 1. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. | Spełnia / Nie spełnia |
| 1. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. | Spełnia / Nie spełnia |
| 1. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps. | Spełnia / Nie spełnia |
| 1. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. | Spełnia / Nie spełnia |
| 1. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. | Spełnia / Nie spełnia |
| 1. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps. | Spełnia / Nie spełnia |
| Funkcje Systemu Bezpieczeństwa: |  |
| W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: | Spełnia / Nie spełnia |
| 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. | Spełnia / Nie spełnia |
| 1. Kontrola Aplikacji. | Spełnia / Nie spełnia |
| 1. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. | Spełnia / Nie spełnia |
| 1. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. | Spełnia / Nie spełnia |
| 1. Ochrona przed atakami - Intrusion Prevention System. | Spełnia / Nie spełnia |
| 1. Kontrola stron WWW. | Spełnia / Nie spełnia |
| 1. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. | Spełnia / Nie spełnia |
| 1. Zarządzanie pasmem (QoS, Traffic shaping). | Spełnia / Nie spełnia |
| 1. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). | Spełnia / Nie spełnia |
| 1. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. | Spełnia / Nie spełnia |
| 1. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. | Spełnia / Nie spełnia |
| 1. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system | Spełnia / Nie spełnia |
| Polityki, Firewall |  |
| 1. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. | Spełnia / Nie spełnia |
| 1. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: | Spełnia / Nie spełnia |
| * Translację jeden do jeden oraz jeden do wielu. | Spełnia / Nie spełnia |
| * Dedykowany ALG (Application Level Gateway) dla protokołu SIP. | Spełnia / Nie spełnia |
| 1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. | Spełnia / Nie spełnia |
| 1. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. | Spełnia / Nie spełnia |
| 1. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. | Spełnia / Nie spełnia |
| * Amazon Web Services (AWS). | Spełnia / Nie spełnia |
| * Microsoft Azure | Spełnia / Nie spełnia |
| * Google Cloud Platform (GCP). | Spełnia / Nie spełnia |
| * OpenStack. | Spełnia / Nie spełnia |
| * VMware NSX. | Spełnia / Nie spełnia |
| Połączenia VPN |  |
| 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: | Spełnia / Nie spełnia |
| * Wsparcie dla IKE v1 oraz v2. | Spełnia / Nie spełnia |
| * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). | Spełnia / Nie spełnia |
| * Obsługa protokołu Diffie-Hellman grup 19 i 20. | Spełnia / Nie spełnia |
| * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. | Spełnia / Nie spełnia |
| * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. | Spełnia / Nie spełnia |
| * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. | Spełnia / Nie spełnia |
| * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. | Spełnia / Nie spełnia |
| * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. | Spełnia / Nie spełnia |
| * Mechanizm „Split tunneling” dla połączeń Client-to-Site. | Spełnia / Nie spełnia |
| 1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: | Spełnia / Nie spełnia |
| * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. | Spełnia / Nie spełnia |
| * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. | Spełnia / Nie spełnia |
| * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. | Spełnia / Nie spełnia |
| Routing i obsługa łączy WAN |  |
| 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: | Spełnia / Nie spełnia |
| * Routingu statycznego. | Spełnia / Nie spełnia |
| * Policy Based Routingu. | Spełnia / Nie spełnia |
| * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. | Spełnia / Nie spełnia |
| Funkcje SD-WAN |  |
| 1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. | Spełnia / Nie spełnia |
| 1. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu. | Spełnia / Nie spełnia |
| Zarządzanie pasmem |  |
| 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. | Spełnia / Nie spełnia |
| 1. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. | Spełnia / Nie spełnia |
| 1. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. | Spełnia / Nie spełnia |
| Ochrona przed malware |  |
| 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). | Spełnia / Nie spełnia |
| 1. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. | Spełnia / Nie spełnia |
| 1. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). | Spełnia / Nie spełnia |
| 1. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. | Spełnia / Nie spełnia |
| 1. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. | Spełnia / Nie spełnia |
| 1. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | Spełnia / Nie spełnia |
| Ochrona przed atakami |  |
| 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. | Spełnia / Nie spełnia |
| 1. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. | Spełnia / Nie spełnia |
| 1. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | Spełnia / Nie spełnia |
| 1. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. | Spełnia / Nie spełnia |
| 1. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. | Spełnia / Nie spełnia |
| 1. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. | Spełnia / Nie spełnia |
| 1. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. | Spełnia / Nie spełnia |
| Kontrola aplikacji |  |
| 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. | Spełnia / Nie spełnia |
| 1. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. | Spełnia / Nie spełnia |
| 1. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. | Spełnia / Nie spełnia |
| 1. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. | Spełnia / Nie spełnia |
| 1. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. | Spełnia / Nie spełnia |
| Kontrola WWW |  |
| 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. | Spełnia / Nie spełnia |
| 1. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. | Spełnia / Nie spełnia |
| 1. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. | Spełnia / Nie spełnia |
| 1. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. | Spełnia / Nie spełnia |
| 1. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. | Spełnia / Nie spełnia |
| 1. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. | Spełnia / Nie spełnia |
| 1. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. | Spełnia / Nie spełnia |
| Uwierzytelnianie użytkowników w ramach sesji |  |
| 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: | Spełnia / Nie spełnia |
| * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. | Spełnia / Nie spełnia |
| * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. | Spełnia / Nie spełnia |
| * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. | Spełnia / Nie spełnia |
| 1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. | Spełnia / Nie spełnia |
| 1. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. | Spełnia / Nie spełnia |
| 1. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | Spełnia / Nie spełnia |
| Zarządzanie |  |
| 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. | Spełnia / Nie spełnia |
| 1. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. | Spełnia / Nie spełnia |
| 1. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. | Spełnia / Nie spełnia |
| 1. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. | Spełnia / Nie spełnia |
| 1. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. | Spełnia / Nie spełnia |
| 1. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. | Spełnia / Nie spełnia |
| 1. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. | Spełnia / Nie spełnia |
| Logowanie |  |
| 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. | Spełnia / Nie spełnia |
| 1. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. | Spełnia / Nie spełnia |
| 1. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. | Spełnia / Nie spełnia |
| 1. Musi istnieć możliwość logowania do serwera SYSLOG. | Spełnia / Nie spełnia |
| Certyfikaty |  |
| Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: |  |
| * ICSA lub EAL4 dla funkcji Firewall. | Spełnia / Nie spełnia |
| Serwisy i licencje |  |
| W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: |  |
| a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. | Spełnia / Nie spełnia |
| Gwarancja oraz wsparcie |  |
| 1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | Spełnia / Nie spełnia |
| Rozszerzone wsparcie serwisowe AHB/SOS |  |
| System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. | Spełnia / Nie spełnia |
| * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). | Spełnia / Nie spełnia |
| * Certyfikat ISO 9001 podmiotu serwisującego. | Spełnia / Nie spełnia |
| System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie: • Wsparcie telefoniczne zespołu certyfikowanych inżynierów. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Konfiguracja startowa urządzenia wg ustaleń z zamawiającym. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). • Przygotowanie urządzenia do zdalnej konfiguracji. • Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. • Minimum 5 zdalnych rekonfiguracj systemu w związku ze zmianą środowiska lub wymagań użytkownika. • Minimum dwa razy w roku zdalny przegląd konfiguracji i logów systemu wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. • Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. | Spełnia / Nie spełnia |
| Opisy do wymagań ogólnych |  |
| 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. | Spełnia / Nie spełnia |
| 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. | Spełnia / Nie spełnia |
| Wartość jednostkowa netto w zł | *Wpisać kwotę jednostkową* |
| Wartość jednostkowa brutto w zł | *Wpisać kwotę jednostkową* |

**C)**

|  |  |
| --- | --- |
| **Serwer plików NAS – 1 sztuka**  **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | **Wpisać nazwę lub model:** |

|  |  |  |
| --- | --- | --- |
| Procesor | Czterordzeniowy o taktowaniu co najmniej 2,2 GHz | Spełnia / Nie spełnia |
| Obudowa | Desktop o wymiarach (Wys. x Szer. x Gł.) : 166 X 343 X 243mm | Spełnia / Nie spełnia |
| Pamięć RAM | 8 GB DDR4 ECC (z możliwością rozbudowy do 32GB) | Spełnia / Nie spełnia |
| Ilość obsługiwanych dysków | 8 kieszeni na dyski 3,5" lub 2,5" SATA HDD/SSD  2 kieszenie na dyski M.2 2280 NVMe SSD | Spełnia / Nie spełnia |
| Interfejsy sieciowe | 4 x 1GbE RJ-45 | Spełnia / Nie spełnia |
| Porty | 4 porty USB 3.2 1 gen.  2 porty eSATA | Spełnia / Nie spełnia |
| Wskaźniki LED | Status, Alert, LAN, HDD1 - 8 | Spełnia / Nie spełnia |
| Obsługa RAID | SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 | Spełnia / Nie spełnia |
| Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | Spełnia / Nie spełnia |
| Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych, Sprzętowy moduł szyfrujący | Spełnia / Nie spełnia |
| System Operacyjny | Windows® 7 i nowsze, macOS® 10.12 i nowsze | Spełnia / Nie spełnia |
| Licencja na Kamery IP | Surveillance Station Maksymalna liczba kamer IP: 40, maks. 1 200 kl./s (FPS) przy rozdzielczości 720p (H.264). (W zestawie dwie licencje) | Spełnia / Nie spełnia |
| Protokoły | SMB, AFP, NFS, FTP, WebDAV, CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN™, L2TP) | Spełnia / Nie spełnia |
| Usługi | Serwer VPN, Serwer pocztowy dla kilku domen, Stacja monitoringu, Windows ACL, Time Backup, Integracja z Windows ADS, Firewall, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS,Zarządzanie przez komórkę, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów w obrębie jednej macierzy RAID, Możliwość utworzenia klastru HA, Obsługa klastru High Availability | Spełnia / Nie spełnia |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów, | Spełnia / Nie spełnia |
| Język GUI | Polski | Spełnia / Nie spełnia |
| Gwarancja i serwis | 36 miesięcy gwarancji producenta | Spełnia / Nie spełnia |
| Waga | Maks. 6 KG | Spełnia / Nie spełnia |
| Pobór mocy | Praca maks. 60W / Hibernacja dysków maks. 27W | Spełnia / Nie spełnia |
| System plików | Wewnętrzny: Btrfs, ext4  Zewnętrzny: Btrfs, ext4, ext3, FAT32, NTFS, HFS+, exFAT | Spełnia / Nie spełnia |
| Liczba wolumenów | Do 64 | Spełnia / Nie spełnia |
| Liczba iSCSI Targetów | Do 128 | Spełnia / Nie spełnia |
| Liczba iSCSI LUN | Do 256 | Spełnia / Nie spełnia |
| Liczba kont użytkowników | 2048 | Spełnia / Nie spełnia |
| Liczba grup | 256 | Spełnia / Nie spełnia |
| Liczba udziałów | 512 | Spełnia / Nie spełnia |
| Ilość jednoczesnych połączeń | 1000 dla SMB,NFS,AFP,FTP (2000 z rozbudową pamięci RAM) | Spełnia / Nie spełnia |
| Głośność | Maks. 23 dB (A) | Spełnia / Nie spełnia |
| Chłodzenie | 2 wentylatory (120 × 120 mm) | Spełnia / Nie spełnia |
| Dyski | 4 dyski 4TB SATA, min. 5400RPM, 256MB cache, 1,000,000 MTBF, gwarancja producenta 3 lata, zgodnych z listą kompatybilną podaną przez producenta NAS | Spełnia / Nie spełnia |
| Wartość jednostkowa netto w zł | *Wpisać kwotę jednostkową* | Wartość jednostkowa netto w zł |
| Wartość jednostkowa brutto w zł | *Wpisać kwotę jednostkową* | Wartość jednostkowa brutto w zł |

**D)**

|  |  |
| --- | --- |
| **Switch- 1 sztuka**  **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | **Wpisać nazwę lub model:** |

|  |  |
| --- | --- |
| Przełącznik sieciowy |  |
| W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. |  |
| W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach: |  |
| Parametry fizyczne platformy |  |
| * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. | Spełnia / Nie spełnia |
| * Zasilanie AC 230V. | Spełnia / Nie spełnia |
| * Maksymalny pobór mocy: 60 W. | Spełnia / Nie spełnia |
| * Minimalny zakres temperatury pracy: 0-40ᵒC. | Spełnia / Nie spełnia |
| Interfejsy sieciowe - wymagania minimalne |  |
| 1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: | Spełnia / Nie spełnia |
| a) 48 porty GE RJ-45. | Spełnia / Nie spełnia |
| e) 4 porty 10 GE SFP+. | Spełnia / Nie spełnia |
| Zarządzanie |  |
| * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). | Spełnia / Nie spełnia |
| * Wsparcie dla SNMP w wersjach 1-3 | Spełnia / Nie spełnia |
| * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. | Spełnia / Nie spełnia |
| * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. | Spełnia / Nie spełnia |
| * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. | Spełnia / Nie spełnia |
| * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). | Spełnia / Nie spełnia |
| * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. | Spełnia / Nie spełnia |
| * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. | Spełnia / Nie spełnia |
| * Automatycznie wykonywane rewizje konfiguracji. | Spełnia / Nie spełnia |
| Parametry wydajnościowe |  |
| * Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. | Spełnia / Nie spełnia |
| * Tablica adresów MAC o pojemności co najmniej 32k wpisów. | Spełnia / Nie spełnia |
| * Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. | Spełnia / Nie spełnia |
| Wymagane funkcje |  |
| * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. | Spełnia / Nie spełnia |
| * Obsługa Jumbo Frames. | Spełnia / Nie spełnia |
| * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). | Spełnia / Nie spełnia |
| * Agregacja portów zgodna ze standardem 802.3ad. | Spełnia / Nie spełnia |
| * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. | Spełnia / Nie spełnia |
| * Obsługa routingu statycznego. | Spełnia / Nie spełnia |
| * Port-mirroring. | Spełnia / Nie spełnia |
| * Uwierzytelnianie 802.1x na poziomie portu. | Spełnia / Nie spełnia |
| * Uwierzytelnianie 802.1x w oparciu o adres MAC. | Spełnia / Nie spełnia |
| * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). | Spełnia / Nie spełnia |
| * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. | Spełnia / Nie spełnia |
| * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. | Spełnia / Nie spełnia |
| * Obsługa protokołu sFlow. | Spełnia / Nie spełnia |
| Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC |  |
| 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: | Spełnia / Nie spełnia |
| * Centralne zarządzanie konfiguracją urządzenia | Spełnia / Nie spełnia |
| * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania | Spełnia / Nie spełnia |
| * Centralne zarządzanie sieciami VLAN. | Spełnia / Nie spełnia |
| * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u | Spełnia / Nie spełnia |
| * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. | Spełnia / Nie spełnia |
| * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. | Spełnia / Nie spełnia |
| * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. | Spełnia / Nie spełnia |
| * Automatyczna detekcja i rekomendacje konfiguracji. | Spełnia / Nie spełnia |
| * Przesyłanie logów na zewnętrzny serwer syslog. | Spełnia / Nie spełnia |
| * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. | Spełnia / Nie spełnia |
| * Obsługa białych i czarnych list adresów MAC. | Spełnia / Nie spełnia |
| * Wykrywanie aplikacji komunikujących się w sieci. | Spełnia / Nie spełnia |
| 1. Musi być możliwe redundantne połączenie z elementami zarządzającymi. | Spełnia / Nie spełnia |
| 1. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. | Spełnia / Nie spełnia |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa |  |
| * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. | Spełnia / Nie spełnia |
| * System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. | Spełnia / Nie spełnia |
| Gwarancja oraz wsparcie |  |
| 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | Spełnia / Nie spełnia |
| 1. Wsparcie telefoniczne. • Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. • Konfiguracja urządzenia wg ustaleń z zamawiającym. • Doradztwo w zakresie konfiguracji. • Zdalne wsparcie techniczne. • Pomoc w zakładaniu zgłoszeń serwisowych u producenta. • Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). • Przygotowanie urządzenia do zdalnej konfiguracji. | Spełnia / Nie spełnia |
| Opisy do wymagań ogólnych |  |
| 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. | Spełnia / Nie spełnia |
| 1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. | Spełnia / Nie spełnia |
| Wartość jednostkowa netto w zł | *Wpisać kwotę jednostkową* |
| Wartość jednostkowa brutto w zł | *Wpisać kwotę jednostkową* |

**E)**

|  |  |
| --- | --- |
| **Zasilanie awaryjne- UPS – 1 sztuka**  WYMAGANE MINIMALNE PARAMETRY TECHNICZNE | **Wpisać nazwę lub model:** |

|  |  |  |
| --- | --- | --- |
| **UPS 3000W (parametry minimalne)** |  |  |
| **Parametr** | **Wymagania minimalne** |  |
| Moc pozorna | minimum 3000VA | Spełnia / Nie spełnia |
| Moc rzeczywista | minimum 3000W | Spełnia / Nie spełnia |
| Technologia | on-line (VFI), podwójna konwersja | Spełnia / Nie spełnia |
| Sprawność max (dla VFI) | ˃ 90 % | Spełnia / Nie spełnia |
| Typ obudowy | rack/tower | Spełnia / Nie spełnia |
| Ilość wydzielanego ciepła dla nominalnych warunków pracy | < 1200 BTU / h | Spełnia / Nie spełnia |
| **praca sieciowa** |  |  |
| Napięcie wejściowe | 110 ÷ 300 V AC ± 5% | Spełnia / Nie spełnia |
| Częstotliwość napięcia wejściowego | 50 / 60 Hz | Spełnia / Nie spełnia |
| Zakres napięcia wyjściowego | 208 V AC / 220 V AC / 230 V AC / 240 V AC ± 1 % | Spełnia / Nie spełnia |
| Wartość napięcia wyjściowego ustawiana z panelu LCD | tak | Spełnia / Nie spełnia |
| Kształt napięcia wyjściowego | sinusoidalny | Spełnia / Nie spełnia |
| Czas przełączania sieć – UPS | 0ms | Spełnia / Nie spełnia |
| Współczynnik odkształceń prądu wejściowego THDi | < 10% | Spełnia / Nie spełnia |
| **praca bateryjna** |  |  |
| Napięcie wyjściowe | ~230V | Spełnia / Nie spełnia |
| Częstotliwość napięcia wyjściowego | 50Hz/60Hz ± 0,5Hz | Spełnia / Nie spełnia |
| Kształt napięcia wyjściowego na pracy bateryjnej | sinusoidalny | Spełnia / Nie spełnia |
| Zabezpieczenie przeciwzwarciowe gniazd wyjściowych | Bezpiecznik automatyczny 16 A | Spełnia / Nie spełnia |
| Zabezpieczenie przeciążeniowe | elektroniczne | Spełnia / Nie spełnia |
| Akumulatory wewnętrzne w UPS / w Module Bateryjnym | minimum 12V 9Ah; szczelne, bezobsługowe | Spełnia / Nie spełnia |
| Czas podtrzymania (100 % Pmax) – przy zastosowaniu baterii wewnętrznych lub z zewętrznym modułem bateryjnym. | Minimum 13 minut | Spełnia / Nie spełnia |
| **pozostałe** |  |  |
| Przeciążalność | 110 % ÷ 120 % = 60s, >120 % = 100ms | Spełnia / Nie spełnia |
| Wejście zasilania | 1 x IEC 320 C20 (16 A) | Spełnia / Nie spełnia |
| Typ i ilość gniazd wyjściowych | min 8x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16 A), z czego minimum 4 gniazda sterowalne | Spełnia / Nie spełnia |
| Sygnalizacja | Wyświetlacz LCD | Spełnia / Nie spełnia |
| Test baterii | wymagana możliwość uruchomienia testu baterii przyciskiem na obudowie zasilacza | Spełnia / Nie spełnia |
| Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych | Wymagana możliwość podłączenia do 10 zewnętrznych modułów bateryjnych | Spełnia / Nie spełnia |
| Możliwość pracy w trybie konwertera częstotliwości | wymagane | Spełnia / Nie spełnia |
| Interfejs komunikacyjny | RS232, USB HID | Spełnia / Nie spełnia |
| Możliwość zainstalowania karty SNMP | wymagane | Spełnia / Nie spełnia |
| Przewody | min 1szt USB + 2szt IEC 320 C13-C14 10A + 1szt IEC 320 C19-C20 16A | Spełnia / Nie spełnia |
| Remote ON/OFF – możliwość zdalnego załączenia/wyłączenia zasilacza | wymagane | Spełnia / Nie spełnia |
| Złącze EPO | wymagane ustawienie NC | Spełnia / Nie spełnia |
| Waga UPS | do 30kg | Spełnia / Nie spełnia |
| Waga MODUŁU BATERYJNEGO – jeżeli występuje | do 42kg | Spełnia / Nie spełnia |
| Wymiary UPS – wersja TOWER | nie większe niż: wysokość 439mm; szerokość 88mm; głębokość 611mm | Spełnia / Nie spełnia |
| Wymiary MODUŁ BATERYJNY – wersja TOWER, jeżeli występuje | nie większe niż: wysokość 439mm; szerokość 88mm; głębokość 611mm | Spełnia / Nie spełnia |
| Gwarancja | minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory; | Spełnia / Nie spełnia |
| Serwis | autoryzowany serwis producenta zlokalizowany na terenie Polski | Spełnia / Nie spełnia |
| naprawa w czasie nie dłuższym niż 5 dni roboczych | Spełnia / Nie spełnia |
| serwis realizowany w systemie door to door | Spełnia / Nie spełnia |
| Oprogramowanie | oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji Vmware, Hyper-V, Citrix XenServer | Spełnia / Nie spełnia |
| możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPSów | Spełnia / Nie spełnia |
| możliwość zarządzania różnymi UPSami tego samego producenta | Spełnia / Nie spełnia |
| wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. | Spełnia / Nie spełnia |
| Certyfikaty producenta (załączyć do oferty) | ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania; | Spełnia / Nie spełnia |
| deklaracja CE producenta sprzętu | Spełnia / Nie spełnia |
| Oświadczenia / dokumenty | oświadczenie producenta o spełnieniu inimalnych wymaganych parametrów specyfikacji | Spełnia / Nie spełnia |
| karta katalogowa oferowanego sprzętu | Spełnia / Nie spełnia |
|  |  |  |

|  |  |
| --- | --- |
| Wartość jednostkowa netto w zł | *Wpisać kwotę jednostkową* |
| Wartość jednostkowa brutto w zł | *Wpisać kwotę jednostkową* |

**F)**

|  |  |
| --- | --- |
| **Pakiet programowania biurowego – 9 szt.**  **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | **Wpisać nazwę lub model:** |

|  |  |  |
| --- | --- | --- |
| Oprogramowanie biurowe | Zintegrowany pakiet aplikacji biurowych pochodzących od jednego producenta, w którego skład ma wchodzić min.:  - edytor tekstów;  - arkusz kalkulacyjny;  - narzędzie do przygotowania i prowadzenia prezentacji;  - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);  - pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim.  - powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa,  przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.  - dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego  - publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.  - możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).  Edytor tekstów musi umożliwiać:  - Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.  - Wstawianie oraz formatowanie tabel.  - Wstawianie oraz formatowanie obiektów graficznych.  - Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  - Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.  - Automatyczne tworzenie spisów treści.  - Formatowanie nagłówków i stopek stron.  - Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.  - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  - Określenie układu strony (pionowa/pozioma).  - Wydruk dokumentów.  - Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Arkusz kalkulacyjny musi umożliwiać:  - Tworzenie raportów tabelarycznych –  - Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych –  - Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.  - Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)  - Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.  - Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych –  - Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych  - Wyszukiwanie i zamianę danych  - Wykonywanie analiz danych przy użyciu formatowania warunkowego  - Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie  - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności  - Formatowanie czasu, daty i wartości finansowych z polskim formatem  - Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  - Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego  - Drukowanie w formacie umożliwiającym robienie notatek –  - Zapisanie jako prezentacja tylko do odczytu.  - Nagrywanie narracji i dołączanie jej do prezentacji  - Opatrywanie slajdów notatkami dla prezentera  - Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo  - Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego  - Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym  - Możliwość tworzenia animacji obiektów i całych slajdów  - Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  - Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego, -  - Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych, -  - Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,  - Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną, -  - Automatyczne grupowanie poczty o tym samym tytule,  - Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,  - Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,  - Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,  - Zarządzanie kalendarzem, -  - Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,  - Przeglądanie kalendarza innych użytkowników,  - Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,  - Zarządzanie listą zadań,  - Zlecanie zadań innym użytkownikom, -  - Zarządzanie listą kontaktów, -  - Udostępnianie listy kontaktów innym użytkownikom,  - Przeglądanie listy kontaktów innych użytkowników,  - Możliwość przesyłania kontaktów innym użytkowników. | Spełnia / Nie spełnia |

|  |  |
| --- | --- |
| Wartość jednostkowa netto w zł | *Wpisać kwotę jednostkową* |
| Wartość jednostkowa brutto w zł | *Wpisać kwotę jednostkową* |

**Łączna cena za dostawę:**

**CZĘŚĆ I**

1. Komputer All-in-One – 9 sztuk
2. Urządzenie UTM – 1 sztuka
3. Serwer plików NAS – 1 sztuka
4. Switch – 1 sztuki
5. Zasilanie awaryjne- UPS – 1 sztuk
6. Pakiet oprogramowanie biurowego – 9 sztuk

wynosi………………………..zł netto + podatek Vat = brutto………………..zł za całość zamówienia (słownie brutto…………………………………………………………………………………)

**Oświadczam, iż:**

1. Zaoferowana cena obejmuje wszelkie koszty związane z realizacją przedmiotu zamówienia, w tym transport
2. Oświadczamy, że oferowany przedmiot zamówienia jest kompletny i będzie gotowy do użytkowania bez żadnych dodatkowych zakupów i inwestycji.
3. Przedmiot zamówienia wykonamy/dostarczymy w terminie do 30 dni kalendarzowych od dnia podpisania umowy
4. Uważamy się za związanych niniejszą ofertą na okres 30 dni
5. Zapoznaliśmy się z postanowieniami zawartymi w zapytaniu ofertowym i zobowiązujemy się, w przypadku wyboru naszej oferty jako najkorzystniejszej, do zrealizowania zamówienia.
6. Zapoznaliśmy się z klauzulą dotyczącą przetwarzania danych osobowych zamieszczoną w Zapytania ofertowym

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

/data, miejscowość/ /podpis i pieczątka imienna

upoważnionego przedstawiciela Wykonawcy/

**ZAŁĄCZNIK NR 1**

**Do zapytania ofertowego**

**...................................................**

Miejscowość data

**FORMULARZ CENOWO – OFERTOWY**

**Część II**

|  |  |
| --- | --- |
| **Nazwa Wykonawcy**  (pieczęć firmowa) |  |
| **Adres siedziby Wykonawcy** |  |
| **NIP Wykonawcy** |  |
| **Telefon do Wykonawcy** |  |
| **E-mail do Wykonawcy** |  |
| **Osoba do kontaktu**  (Imię i nazwisko oraz dane kontaktowe) |  |

***Odpowiadając na zapytanie ofertowe z dnia 28.04.2023 pn.: „Dostawa sprzętu komputerowego w ramach projektu grantowego „Cyfrowa Gmina” realizowanego w ramach POPC 2014-2020”, oferuję wykonać / dostarczyć przedmiot zamówienia, na warunkach określonymi poniżej:***

**CZĘŚĆ II**

A) Oprogramowania serwera bazy danych - 1szt. (30 użytkowników)

Przedmiotem zamówienia jest dostawa oprogramowania Microsoft SQL Server 2022 w wersji najnowszej lub oprogramowania równoważnego.

Zakup licencji bezterminowej na system bazodanowy i 30 licencji dla użytkowników systemu bazodanowego. System ten musi obsługiwać minimum 8 rdzeni oraz 64 GB pamięci RAM. Licencja powinna umożliwiać wykorzystywanie systemu na maszynie fizycznej lub wirtualnej.

|  |  |
| --- | --- |
| Oprogramowania serwera bazy danych - **1 sztuka**  **WYMAGANE MINIMALNE PARAMETRY TECHNICZNE** | **Wpisać nazwę lub model:** |

|  |  |
| --- | --- |
| Wartość jednostkowa netto w zł | *Wpisać kwotę jednostkową* |
| Wartość jednostkowa brutto w zł | *Wpisać kwotę jednostkową* |

**Łączna cena za dostawę:**

A) Oprogramowania serwera bazy danych - 1 sztuka

wynosi………………………..zł netto + podatek Vat = brutto………………..zł za całość zamówienia (słownie brutto…………………………………………………………………………………)

**Oświadczam, iż:**

1. Zaoferowana cena obejmuje wszelkie koszty związane z realizacją przedmiotu zamówienia, w tym transport
2. Oświadczamy, że oferowany przedmiot zamówienia jest kompletny i będzie gotowy do użytkowania bez żadnych dodatkowych zakupów i inwestycji.
3. Przedmiot zamówienia wykonamy/dostarczymy w terminie do 30 dni kalendarzowych od dnia podpisania umowy
4. Uważamy się za związanych niniejszą ofertą na okres 30 dni
5. Zapoznaliśmy się z postanowieniami zawartymi w zapytaniu ofertowym i zobowiązujemy się, w przypadku wyboru naszej oferty jako najkorzystniejszej, do zrealizowania zamówienia.
6. Zapoznaliśmy się z klauzulą dotyczącą przetwarzania danych osobowych zamieszczoną w Zapytania ofertowym

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

/data, miejscowość/ /podpis i pieczątka imienna

upoważnionego przedstawiciela Wykonawcy/