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

( pieczęć wykonawcy)

* + 1. INFORMACJA O PARAMETRACH TECHNICZNYCH
    2. I TERMINIE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

Ja (My), niżej podpisany (ni)...............................................................................

działając w imieniu i na rzecz :

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

(pełna nazwa wykonawcy)

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

(adres siedziby wykonawcy)

w odpowiedzi na ogłoszenie o przetargu nieograniczonym na:

**"Zakup i dostawę elementów bazy sprzętowo-programowej do cyfrowej archiwizacji części analogowej dokumentacji powiatowego zasobu geodezyjnego i kartograficznego"**

przedstawiamy informację o parametrach technicznych sprzętu

**1) Urządzenia wielofunkcyjne – 5 sztuk**

**(nazwa i model :……………….....................................…………………………………)**

„Tabelę należy uzupełnić wpisując parametry oferowanego sprzętu lub wpisać słowo „SPEŁNIA”, w przypadku gdy zaoferowany sprzęt odpowiada minimalnym wymaganiom zapisanym w OPZ przygotowanym przez Zamawiającego”.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| 1 | Technologia druku |  |
| 2 | Technologia tonera |  |
| 3 | Szybkość druku |  |
| 4 | Czas oczekiwania na wydruk pierwszej strony kolorowej |  |
| 5 | Czas oczekiwania na wydruk pierwszej strony mono |  |
| 6 | Czas nagrzewania |  |
| 7 | Pamięć RAM |  |
| 8 | Dysk twardy |  |
| 9 | Język wydruku |  |
| 10 | Rozdzielczość wydruku |  |
| 11 | Maksymalne obciążenie miesięczne |  |
| 12 | Kopiowanie wielokrotne |  |
| 13 | Powiększenie |  |
| 14 | Funkcje kopiowania/drukowania |  |
| 15 | Pierwszy podajniki papieru |  |
| 16 | Drugi podajnik papieru |  |
| 17 | Podajnik papieru ręczny |  |
| 18 | Dodatkowe podajniki papieru |  |
| 19 | Podajnik oryginałów |  |
| 20 | Pojemność odbiorcza |  |
| 21 | Prędkość skanowania |  |
| 22 | Rodzaj modułu skanera |  |
| 23 | Rozdzielczość skanowania |  |
| 24 | Tryby skanowania |  |
| 25 | Obsługiwane formaty papieru |  |
| 26 | Obsługiwane formaty papieru w druku/kopiowaniu dwustronnym |  |
| 27 | Obsługiwana gramatura papieru |  |
| 28 | Obsługiwana gramatura papieru w druku/kopiowaniu dwustronnym |  |
| 29 | Interfejsy |  |
| 30 | Obsługiwane protokoły |  |
| 31 | Obsługiwane protokoły sieciowe |  |
| 32 | Wsparcie systemów operacyjnych |  |
| 33 | Zasilanie |  |
| 34 | Wyświetlacz |  |
| 35 | Język menu |  |
| 36 | Startowe materiały eksploatacyjne |  |
| 37 | Możliwość podłączenia wewnętrznego czytnika zbliżeniowych kart identyfikacyjnych oraz zewnętrznej klawiatury |  |
| 38 | Wbudowana przeglądarka |  |
| 39 | Obsługa Apple Airprint 1.4 |  |
| 40 | Wbudowana możliwość rozpoznawania polskiego tekstu OCR i skanowania do przeszukiwalnego PDF |  |
| 41 | Dodatkowa szuflada na dokumenty i materiały eksploatacyjne będąca podstawą urządzenia umożliwiająca jego mobilność |  |
| 42 | Certyfikaty |  |
| 43 | Czcionki wbudowane |  |
| 44 | Gwarancja i rękojmia |  |

**2) System ochrony sieci**

**(nazwa i model :……………….....................................…………………………………)**

Tabelę należy uzupełnić wpisując słowo „SPEŁNIA”, w przypadku gdy zaoferowany sprzęt odpowiada minimalnym wymaganiom zapisanym w OPZ przygotowanym przez Zamawiającego”.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry** |
| 1. | System zabezpieczeń musi być zbudowany w oparciu o dedykowane rozwiązania sprzętowe (tzw. appliance). |  |
| 2. | System zabezpieczeń musi zapewniać możliwość rozbudowy w przyszłości o kolejne urządzenie i pracę w klastrze w trybie Active-Passive. |  |
| 3. | Elementy systemu przenoszące ruch użytkowników musi dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub bridge. |  |
| 4. | System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000. |  |
| 5. | System musi dysponować minimum 1 portem USB. |  |
| 6. | System musi umożliwiać tworzenie minimum 256 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. |  |
| 7. | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). * Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP). * Poufność danych - IPSec VPN oraz SSL VPN. * Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]. * Kontrola stron internetowych – Web Filter [WF]. * Kontrola pasma oraz ruchu [QoS i Traffic shaping]. * Kontrola aplikacji oraz rozpoznawanie ruchu P2P. * Możliwość analizy ruchu szyfrowanego SSL’em. |  |
| 8. | Wydajność systemu Firewall minimum 8 000 Mbps. |  |
| 9. | W zakresie Firewall’a obsługa nie mniej niż 2 500 000 jednoczesnych połączeń oraz 60 000 nowych połączeń na sekundę. |  |
| 10. | Wydajność skanowania strumienia danych przy włączonych funkcjach: antywirus minimum 2 200 Mbps. |  |
| 11. | Wydajność ochrony przed atakami (IPS) minimum 2 500 Mbps. |  |
| 12. | Wydajność szyfrowania AES, nie mniej niż 1 000 Mbps. |  |
| 13. | WW zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:   * Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Obsługa mechanizmów: IPSec NAT Traversal, DPD. |  |
| 14. | Rozwiązanie musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIP, OSPF, BGP. |  |
| 15. | Translacja adresów NAT adresu źródłowego i NAT adresu docelowego. |  |
| 16. | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i priorytety). |  |
| 17. | System zabezpieczeń musi wspierać obsługę modemów 3G. Modemy powinny pochodzić od dowolnie wybranych producentów. |  |
| 18. | System zabezpieczeń musi umożliwiać tworzenie wydzielonych stref bezpieczeństwa Firewall np. DMZ. |  |
| 19. | System musi umożliwiać automatyczne przełączanie na inne łącze w przypadku awarii podstawowego łącza. System musi wspierać podłączenie co najmniej trzech niezależnych łącz. |  |
| 20. | W ramach ochrony IPS system musi:   * Opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać, co najmniej 4000 wpisów. * Pozwalać na definiowanie własnych wyjątków lub sygnatur. * Wykrywać anomalie protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. * Generować alerty w przypadku prób ataków. |  |
| 21. | W zakresie kontroli aplikacji oraz rozpoznawania ruchu P2P wymagane jest co najmniej:   * Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza rozpoznawanych aplikacji musi zawierać co najmniej 2000 wpisów. * Blokowanie komunikatorów internetowych przynajmniej: Gadu-Gadu, Skype, Facebook Chat). * Blokowanie mediów strumieniowych przynajmniej: YouTube, radio internetowe. * Blokowanie uruchamiania aplikacji i gier w serwisie Facebook. * Blokowanie aplikacji proxy przynajmniej: TOR, Ultrasurf, JAP. * Blokowanie aplikacji P2P przynajmniej: BitTorrent, uTorrent, eMule. |  |
| 22. | W zakresie kontroli stron internetowych system musi:   * Zapewniać bazę filtra WWW pogrupowanych w kategorie tematyczne – minimum 40 kategorii. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. * Umożliwiać definiowanie polityk dostępu do stron internetowych w oparciu o harmonogramy czasowe dla użytkowników i grup użytkowników. * Wyświetlać komunikat użytkownikom wyjaśniający powód zablokowania dostępu do strony internetowej. Administrator musi mieć możliwość personalizacji treści komunikatu i dodania logo organizacji. * Umożliwiać przydzielanie polityki QoS dla kategorii stron internetowych np. portale społecznościowe. |  |
| 23. | Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych. |  |
| 24. | System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:   * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory. |  |
| 25. | Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikaty:   * ICSA lub EAL4 – dla funkcjonalności Firewall. |  |
| 26. | System bezpieczeństwa musi być wyposażony w dysk twardy (minimum 120 GB) do celów lokalnego przechowywania logów i generowania raportów. Nie dopuszcza się składowania logów poza organizacją lub w chmurze. |  |
| 27. | System bezpieczeństwa musi zawierać moduł logowania zdarzeń i raportowania. Moduł logowania zdarzeń i raportowania może być realizowany w postaci osobnej platformy sprzętowej lub programowej. W ramach modułu raportowania system musi zapewniać:   * Składowanie oraz archiwizację logów * Gromadzenie informacji o zdarzeniach dotyczących ruchu Web, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz powiązanie ich z nazwami użytkowników * Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących * Generowanie i eksport raportów do plików HTML i PDF * Eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych) |  |
| 28. | Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |  |
| 29. | W ramach zarządzania system bezpieczeństwa musi:   * Umożliwiać tworzenie kont administracyjnych o różnych uprawnieniach. * Umożliwiać określanie złożoności polityk hasłowych dla administratorów. * Wspierać SNMP. * Monitorować na bieżąco stan urządzenia (obciążenie interfejsów sieciowych, CPU, pamięć RAM). * Przechowywać przynajmniej dwie wersji firmware. * Wykonywać automatycznie kopie zapasowe konfiguracji systemu. |  |
| 30. | Dostawca musi dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa: antywirus, antyspam, IPS, kontrola stron internetowych, kontrola aplikacji sieciowych na okres 36 miesięcy. |  |
| 31. | System bezpieczeństwa musi być objęty gwarancją i rękojmią producenta na okres 36 miesięcy w trybie NBD (next business day). |  |
| 32 | W okresie gwarancji cza reakcji serwisu od momentu zgłoszenia usterki w ciągu 1 dnia roboczego. |  |

**3) Sprzęt do rozbudowy macierzy dyskowej HP 3PAR 7200**

**(nazwa, model i numer seryjny :………………............................................……………)**

**4) Oprogramowanie do katalogowania zeskanowanych plików PDF**

Tabelę należy uzupełnić wpisując słowo „SPEŁNIA”, w przypadku gdy zaoferowany sprzęt odpowiada minimalnym wymaganiom zapisanym w OPZ przygotowanym przez Zamawiającego”.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry** |
| 1. | Praca w środowisku zgodnym z systemami Microsoft Windows od wersji 7 wzwyż. |  |
| 2. | Oprogramowanie wykonane w technologii .NET i MS-SQL lub innej podobnej. |  |
| 3. | Aplikacja powinna być zintegrowana ze środowiskiem AD w celu pobierania uprawnień do jej obsługi. |  |
| 4. | Obsługa z klasycznego okienkowego interfejsu użytkownika. Nie dopuszcza się obsługi z okna przeglądarki internetowej. |  |
| 5. | Oprogramowanie ma katalogować pliki PDF na podstawie informacji z OCR, umieszczać w bazie danych i podpisywać certyfikatem z wskazanego CA. |  |
| 6. | Aplikacja powinna logować zdarzenia i transakcje w dowolnej lokalizacji. |  |
| 7. | Aplikacja powinna umożliwiać robienie kopii zapasowych konfiguracji i danych, |  |
| 8. | Wraz z aplikacją ma być przekazany autorskie prawa majątkowe i oraz kod źródłowy. |  |
| 9. | Wsparcie producenta i gwarancja 12 m-cy, |  |
| 10. | Czas reakcji serwisu na podjęcie naprawy gwarancyjnej w terminie 3 dni roboczych od daty zgłoszenia |  |
| 11 | Przeszkolenie z obsługi w siedzibie zamawiającego. |  |

**5) Kryterium - termin realizacji zamówienia.**

Tabelę należy uzupełnić wpisując słowo „TAK”, przy wybranym podkryterium.

|  |  |  |
| --- | --- | --- |
| Lp. | Podkryterium oceny ofert w  kryterium "termin realizacji" | oferowany termin realizacji jako kryterium oceny ofert |
| 1 | do 8 tygodni od daty podpisania umowy |  |
| 2 | do 9 tygodni od daty podpisania umowy |  |
| 3 | do 10 tygodni od daty podpisania umowy |  |

..............................., dn. ............................... ….........................................................................

(podpis(y) osób uprawnionych do reprezentacji wykonawcy, w przypadku oferty wspólnej- podpis pełnomocnika wykonawców