**Załącznik Nr 4 do SWZ – Opis przedmiotu zamówienia.**

**Numer sprawy: PiPR.IV.272.9.2022**

**„Zakup i dostawa urządzeń i oprogramowania cyfrowego w ramach projektu Cyfrowy Powiat”**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest„Zakup i dostawa urządzeń i oprogramowania cyfrowego w ramach projektu Cyfrowy Powiat” w podziale na części:

**I część:** Zakup i dostawa urządzeń cyfrowych – zestawów komputerowych

**II część:** Zakup i dostawa urządzeń cyfrowych – UTM wraz z dwoma punktami dostępowymi wi-fi.

**III część:** Zakup i dostawa systemu urządzeń cyfrowych – cyfrowego zarządzania dokumentacją – oprogramowanie.

1. **SZCZEGÓŁOWY OPIS CZĘŚCI I:**
2. Przedmiotem zamówienia jest zakup i dostawa zestawów komputerowych w następujących konfiguracjach:

konfiguracja I.I.: Trzy zestawy komputerowe o konfiguracji – komputer stacjonarny i dwa monitory.

konfiguracja I.II.: Trzy zestawy komputerowe o konfiguracji – komputer stacjonarny i monitor.

konfiguracja I.I. **Trzy zestawy** komputerowe o konfiguracji –**komputer stacjonarny i dwa monitory**, o poniższych parametrach:

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Procesor  | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 12300 punktów, według wyników ze strony <https://www.cpubenchmark.net>  |
| Pamięć RAM | 8GB DDR4 możliwość rozbudowy do min 64GB, min. 1 slot wolny |
| Pamięć masowa | 512 GB SSD PCIe NVMe |
| Karta graficzna  | Zintegrowana z procesorem / Dedykowana karta graficzna z min. 2GB RAM, złącza DVI, HDMI |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, port audio combo ( słuchawki + mikrofon ) na panelu przednim, na panelu tylnym złącze audio out |
| Obudowa | Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęce zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 700mm, waga max 6kg,Zasilacz o mocy max. 260W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Wbudowany w zasilaczu system diagnostyczny do sprawdzenia zasilacza bez konieczności włączania komputera, Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER (tzn. zmiana barw i miganie); w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora.Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnęk zewnętrznych oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego.Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Zgodność z systemem operacyjnym | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi |
| Bezpieczeństwo | Ukryty w laminacie płyty głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS lub w menu boot’owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do internetu, braku dostępu do sieci, bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.  |
| BIOS  | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, dacie wysyłki komputera z fabryki, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora,ilości rdzeni zainstalowanego procesora, typowej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej,Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Możliwość wyłączania portów USB w tym:- tylko portów USB znajdujących się na przednim panelu obudowy, - tylko portów USB znajdujących się na tylnym panelu obudowy.- wszystkich portów USB- pojedynczo  |
| Certyfikaty i standardy | Urządzenia muszą być produkowane są przez producenta, zgodnie z normą IO9001 oraz ISO 50001 (certyfikaty załączyć do oferty) |
| Oprogramowanie  | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi być zapisany trwale w BIOS oraz Office Home and Business 2021 (PL) |
| Wymagania dodatkowe: | Wbudowane porty: - panel przedni : 2x USB 3.2 gen 1,2x USB 2.0, 1x audio (dopuszcza się combo),- panel tylny: 1x audio out,2x USB 3.2 gen 1, 2x USB 2.0, 1x VGA, 1x HDMI, 1x RJ45Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : 1x PCI Express x16 Gen.3, 1x PCI Express x1, min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza SATA w tym 1 szt SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFIKarta sieci bezprzewodowej 802.11 ac + bluetoothWbudowany napęd DVD +/- RWKlawiatura USB w układzie polski programisty Mysz USB z klawiszami oraz rolką (scroll) |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 26 dB – załączyć oświadczenie producenta |
| Warunki gwarancji | 3-letnia gwarancja producenta świadczona na miejscu u klienta, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną producentaCzas reakcji serwisu - do końca następnego dnia roboczegoWymagane dołączenie do oferty oświadczenie Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
| Wsparcie techniczne producenta | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |

|  |  |
| --- | --- |
| Nazwa komponentu | Minimalne wymagane parametry techniczne monitorów |
| Proporcje obrazu | 16:9 |
| Przekątna ekranu | 23.6" |
| Typ matrycy | AMVA+ |
| Technologia podświetlania | Diody LED |
| Obszar widzialny w pionie | 293 mm |
| Obszar widzialny w poziomie | 521 mm |
| Plamka matrycy | 0.2715 mm |
| Rozdzielczość | 1920 x 1080 (FHD 1080) |
| Czas reakcji | 6 ms |
| Jasność | 250 cd/m² |
| Kontrast statyczny | 3 000:1 |
| Kontrast dynamiczny | 12 000 000:1 |
| Częstotliwość pozioma min. | 24 kHz |
| Częstotliwość pozioma max. | 80 kHz |
| Częstotliwość pionowa min. | 56 Hz |
| Częstotliwość pionowa max. | 75 Hz |
| Kąt widzenia poziomy | 178 ° |
| Kąt widzenia pionowy | 178 ° |
| Ilość kolorów | 16,7 mln |
| Gniazda we/wy | 1 x 15-pin D-Sub |
| 1 x DVI-D |
| 1 x HDMI |
| Wbudowane głośniki | Tak |
| Pivot | Tak |
| Certyfikaty | CE |
| TCO |
| TUV |
| Standard VESA | 100 x 100 |
| Pobór mocy | 26 W |
| Akcesoria w zestawie | - Kabel zasilający |
| - Kabel DVI-D, HDMI |
| - Kabel Audio |
| - Stopka |
| - Podstawa stopki |
| - Uchwyt na kable |
| - Skrócona instrukcja obsługi |
| - Instrukcja bezpieczeństwa |
| Kolor | Czarny |
| Wysokość | maksymalnie 537 mm |
| Szerokość | maksymalnie 545 mm |
| Głębokość | maksymalnie 230 mm |
| Waga | maksymalnie 5.5 kg |
| Gwarancja | 36 miesięcy producenta |
| Pozostałe parametry | - Synchronizacja: separate sync |
| - 5 przycisków obsługi |
| - Głośniki 2x 2W (Stereo) |
| - Stopka z regulacją wysokości (130 mm) |
| - Obrót ekranu: 90 stopni |
| - Kąt obrotu: 320 stopni, 160 w lewo i 160 w prawo |
| - Kąt pochylenia: 22 stopni w górę i 5 stopni w dół |
| - Zasilacz wewnętrzny: AC 100-240V 50/60Hz |

konfiguracja I.II.: **Trzy zestawy** komputerowe o konfiguracji – **komputer stacjonarny i monitor**, o poniższych parametrach:

|  |  |
| --- | --- |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
| Typ | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| Zastosowanie | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| Procesor  | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 12300 punktów, według wyników ze strony <https://www.cpubenchmark.net>  |
| Pamięć RAM | 8GB DDR4 możliwość rozbudowy do min 64GB, min. 1 slot wolny |
| Pamięć masowa | 512 GB SSD PCIe NVMe |
| Karta graficzna  | Zintegrowana z procesorem  |
| Wyposażenie multimedialne | Karta dźwiękowa zintegrowana z płytą główną, port audio combo ( słuchawki + mikrofon) na panelu przednim, na panelu tylnym złącze audio out |
| Obudowa | Typu SFF z obsługą kart rozszerzeń o niskim profilu, napęd optyczny w dedykowanej wnęce zewnętrznej slim. Suma wymiarów mierzona po krawędziach obudowy nie może przekraczać 700mm, waga max 6kg,Zasilacz o mocy max. 260W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, Wbudowany w zasilaczu system diagnostyczny do sprawdzenia zasilacza bez konieczności włączania komputera, Obudowa musi posiadać wbudowany wizualny system diagnostyczny, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami, sygnalizacja oparta na zmianie statusów diody LED np. przycisku POWER (tzn. zmiana barw i miganie); w szczególności musi sygnalizować: uszkodzenie lub brak pamięci RAM, uszkodzenie płyty głównej, awarię procesora.Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wnęk zewnętrznych oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego.Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| Zgodność z systemem operacyjnym | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi |
| Bezpieczeństwo | Ukryty w laminacie płyty głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS lub w menu boot’owania system diagnostyczny z graficznym interfejsem użytkownika, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność: test procesora, test pamięci, test wentylatora dla procesora, test dysku twardego. System diagnostyczny działający w przypadku braku dysku, uszkodzenia, utraty wszystkich partycji, braku dostępu do internetu, braku dostępu do sieci, bez podłączania zewnętrznych oraz wewnętrznych urządzeń np. pamięć flash USB itp.  |
| BIOS  | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, nazwę producenta komputera, model komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych oraz dodatkowego oprogramowania typu system diagnostyczny odczytania z wewnętrznego menu BIOS informacji o: wersji BIOS, nr seryjnym komputera, dacie wyprodukowania komputera, dacie wysyłki komputera z fabryki, ilości zainstalowanej pamięci RAM, prędkości zainstalowanych pamięci RAM, technologii wykonania pamięci, sposobie obsadzeniu slotów pamięci z rozbiciem na wielkości pamięci i banki, typie zainstalowanego procesora,ilości rdzeni zainstalowanego procesora, typowej, minimalnej i maksymalnej prędkości zainstalowanego procesora, pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adresie zintegrowanej karty sieciowej,Funkcja blokowania wejścia do BIOS oraz blokowania startu systemu operacyjnego, (gwarantujący utrzymanie zapisanego hasła nawet w przypadku odłączenia wszystkich źródeł zasilania i podtrzymania BIOS)Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.Możliwość ustawienia hasła systemowego/użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Możliwość wyłączania portów USB w tym:- tylko portów USB znajdujących się na przednim panelu obudowy, - tylko portów USB znajdujących się na tylnym panelu obudowy.- wszystkich portów USB- pojedynczo  |
| Certyfikaty i standardy | Urządzenia muszą być produkowane są przez producenta, zgodnie z normą IO9001 oraz ISO 50001 (certyfikaty zalączyć do oferty) |
| Oprogramowanie  | Zainstalowany system operacyjny Windows 11 Professional, klucz licencyjny musi być zapisany trwale w BIOS oraz Office Home and Business 2021 (PL) |
| Wymagania dodatkowe: | Wbudowane porty: - panel przedni : 2x USB 3.2 gen 1,2x USB 2.0, 1x audio (dopuszcza się combo),- panel tylny: 1x audio out,2x USB 3.2 gen 1, 2x USB 2.0, 1x VGA, 1x HDMI, 1x RJ45Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w : 1x PCI Express x16 Gen.3, 1x PCI Express x1, min. 2 złącza DIMM z obsługą do 64GB DDR4 pamięci RAM, min. 2 złącza SATA w tym 1 szt SATA 3.0, 1 złącze M.2 dla dysków SSD, 1 złącze M.2 dla bezprzewodowej karty WiFIKarta sieci bezprzewodowej 802.11 ac + bluetoothWbudowany napęd DVD +/- RWKlawiatura USB w układzie polski programisty Mysz USB z klawiszami oraz rolką (scroll) |
| Ergonomia | Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy jałowej dysku twardego (IDLE) wynosząca maksymalnie 26 dB – załączyć oświadczenie producenta |
| Warunki gwarancji | 3-letnia gwarancja producenta świadczona na miejscu u klienta, możliwość zgłaszania awarii przez ogólnopolską linię telefoniczną producentaCzas reakcji serwisu - do końca następnego dnia roboczegoWymagane dołączenie do oferty oświadczenie Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.Firma serwisująca musi posiadać ISO 9001: 2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera. |
| Wsparcie techniczne producenta | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |

|  |  |
| --- | --- |
| Nazwa komponentu | Minimalne wymagane parametry techniczne monitorów |
| Proporcje obrazu | 16:9 |
| Przekątna ekranu | 23.6" |
| Typ matrycy | AMVA+ |
| Technologia podświetlania | Diody LED |
| Obszar widzialny w pionie | 293 mm |
| Obszar widzialny w poziomie | 521 mm |
| Plamka matrycy | 0.2715 mm |
| Rozdzielczość | 1920 x 1080 (FHD 1080) |
| Czas reakcji | 6 ms |
| Jasność | 250 cd/m² |
| Kontrast statyczny | 3 000:1 |
| Kontrast dynamiczny | 12 000 000:1 |
| Częstotliwość pozioma min. | 24 kHz |
| Częstotliwość pozioma max. | 80 kHz |
| Częstotliwość pionowa min. | 56 Hz |
| Częstotliwość pionowa max. | 75 Hz |
| Kąt widzenia poziomy | 178 ° |
| Kąt widzenia pionowy | 178 ° |
| Ilość kolorów | 16,7 mln |
| Gniazda we/wy | 1 x 15-pin D-Sub |
| 1 x DVI-D |
| 1 x HDMI |
| Wbudowane głośniki | Tak |
| Pivot | Tak |
| Certyfikaty | CE |
| TCO |
| TUV |
| Standard VESA | 100 x 100 |
| Pobór mocy | 26 W |
| Akcesoria w zestawie | - Kabel zasilający |
| - Kabel DVI-D, HDMI |
| - Kabel Audio |
| - Stopka |
| - Podstawa stopki |
| - Uchwyt na kable |
| - Skrócona instrukcja obsługi |
| - Instrukcja bezpieczeństwa |
| Kolor | Czarny |
| Wysokość | maksymalnie 537 mm |
| Szerokość | maksymalnie 545 mm |
| Głębokość | maksymalnie 230 mm |
| Waga | maksymalnie 5.5 kg |
| Gwarancja | 36 miesięcy producenta |
| Pozostałe parametry | - Synchronizacja: separate sync |
| - 5 przycisków obsługi |
| - Głośniki 2x 2W (Stereo) |
| - Stopka z regulacją wysokości (130 mm) |
| - Obrót ekranu: 90 stopni |
| - Kąt obrotu: 320 stopni, 160 w lewo i 160 w prawo |
| - Kąt pochylenia: 22 stopni w górę i 5 stopni w dół |
| - Zasilacz wewnętrzny: AC 100-240V 50/60Hz |

1. Produkty powinny być nowe, wyprodukowane w roku 2022, zapakowane przez producenta, dopuszczone do sprzedaży na terenie Polski i posiadać wszystkie opisane w powyższych tabelach wymagania, certyfikaty, normy.

**SZCZEGÓŁOWY OPIS CZĘŚCI II:**

1. Zakup i dostawa urządzeń cyfrowych – UTM wraz z dwoma punktami dostępowymi wi-fi.
2. Ogólny opis systemu:

# Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę 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.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

# Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

# Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 2 gniazdami SFP+ 10 Gbps.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

# Parametry wydajnościowe:

1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps.
5. 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 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

# Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

# Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

# Routing i obsługa łączy WAN

* + 1. W zakresie routingu rozwiązanie zapewnia obsługę:
1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

# Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

# Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# Certyfikaty

Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje:

* ICSA lub EAL4 dla funkcji Firewall.

# Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

# Gwarancja oraz wsparcie

Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

System musi posiadać możliwość obsługi i zarządzania istniejącą w urzędzie siecią punktów dostępowych FortiAp

1. **Access Point dwie sztuki**

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

* 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:

Temperatura 0–50°C,

Wilgotność 5–90%.

* 1. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
	2. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:

2.4 GHz 802.11b/g/n,

5 GHz 802.11a/n/ac/ax,

Skaner 2.4GHz i 5GHz

* 1. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
	2. Urządzenie musi być wyposażone w moduł BLE.
	3. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 10/100/1000 Base-TX,
	4. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.
	5. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:

Tunnel,

Bridge,

Mesh.

* 1. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
	2. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
	3. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:

MIMO – 2x2,

* 1. Maksymalna przepustowość dla poszczególnych modułów radiowych:

574 Mbps;

1201 Mbps;

* 1. Wymagana moc nadawania:

min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;

min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;

* 1. Wsparcie dla 802.11n 20/40Mhz HT,
	2. Wsparcie dla kanałów 80MHz,
	3. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
	4. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
	5. Maksymalna deklarowana liczba klientów per moduł radiowy:

512;

512;

* 1. Funkcje dodatkowe:

OFDMA UL i DL

Spatial Reuse (BSS Coloring)

UL-MU-MIMO 802.11ax

DL-MU-MIMO

Enhanced Target Wake Time (TWT)

# Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 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.

**SZCZEGÓŁOWY OPIS CZĘŚCI III:**

1. Przedmiotem zamówienia jest zakup i dostawa **systemu urządzeń cyfrowych – cyfrowego zarządzania dokumentacją - oprogramowanie** o następujących parametrach:
	1. System REJAKT lub równoważny, oferujący integracje z użytkowanym przez zamawiającego systemem STRATEG
	2. W programie sprawy prowadzone są w ramach sygnatury spraw (zdefiniowanej przez użytkownika) i przedstawione w postaci listy za pomocą czytelnego i przejrzystego interfejsu, który umożliwia jednoczesne przeglądanie atrybutów (parametrów) sprawy, takich jak: data wniosku, data decyzji czy przedmiot sprawy. Do każdej sygnatury można utworzyć zindywidualizowany słownik występujących w sprawie stron zawierający dla każdego charakteru osoby dane istotne z punktu widzenia tworzenia rejestru spraw. Może to być na przykład numer uprawnień projektanta, specjalność czy branża. Ze sprawą powiązane są ponadto pisma powstające w toku postępowania. Program umożliwia przechowywanie treści wniosku (np. skanów) oraz treści pism i decyzji tworzonych w wewnętrznym edytorze pism.
	3. REJAKT (LOK-TER) - Rejestr spraw związanych z lokalizacją terenową, lub równoważny, oferujący integracje z użytkowanym przez zamawiającego systemem STRATEG
	4. REJAKT (POZ-BUD) - Rejestr wniosków o pozwolenie na budowę oraz decyzji o pozwoleniu na budowę, lub równoważny, oferujący integracje z użytkowanym przez zamawiającego systemem STRATEG
	5. REJAKT (WAR-ZAB) - Rejestr decyzji o ustaleniu warunków zabudowy lub równoważny, oferujący integracje z użytkowanym przez zamawiającego systemem STRATEG.

Programy umożliwiają połączenie spraw z obiektami terenowymi zobrazowanymi w EWMAPIE (element systemu STRATEG).

* 1. Numery działek umożliwiają wykonanie wizualizacji na mapie w aplikacji EWMAPA. Poza tym zdefiniowanie numerów działek, których dotyczy postępowanie, daje możliwość automatycznego wczytania z programu EWOPIS nazwisk i adresów osób będących stronami w postępowaniu. Numery działek da się również zaczytać do aplikacji bezpośrednio z mapy. Podczas procedury weryfikacji wniosku w EWMAPIE istnieje możliwość podczytywania (wyświetlenia) danych niezbędnych do jej przeprowadzenia (jeśli istnieją one w systemie), takich jak: studium uwarunkowań i kierunków zagospodarowania, miejscowe plany zagospodarowania przestrzennego, budynki, istniejące uzbrojenie terenu, projektowane uzbrojenie terenu, a także zakresy innych decyzji (np. decyzji o warunkach zabudowy). Wprowadzenie zakresu decyzji w EWMAPIE umożliwia również wykonywanie analiz przestrzennych (np. wygenerowanie zestawienia obszarów studium wchodzących w zakres decyzji wraz z ich powierzchnią).
	2. WINPLAN – plany zagospodarowania przestrzennego, lub równoważny, oferujący integracje z użytkowanym przez zamawiającego systemem STRATEG
	3. Do zakładania oraz bieżącego prowadzenia części opisowej (ustaleń) wszystkich miejscowych planów zagospodarowania przestrzennego. Oprócz przeglądania i modyfikacji danych z poziomu aplikacji można wykonać różnego rodzaju wydruki oraz niezbędne konfiguracje baz i programów interfejsowych. Ściśle współpracuje z graficzną częścią miejscowych planów zagospodarowania

przestrzennego prowadzonych w EWMAPIE, z poziomu której istnieje możliwość odczytania ustaleń dla określonego obszaru miejscowego planu zagospodarowania przestrzennego oraz wykonania wypisu i wyrysu, opierając się na zdeklarowanym przez użytkownika wzorcu. moduł umożliwiający automatyczne utworzenie kolorystyki poszczególnych obszarów planu na podstawie nadanej im funkcji. Eksport zbiorów danych oraz metadanych do formatu GML dostosowanego do wymogów rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 26 października 2020 r. w sprawie zbiorów danych przestrzennych oraz metadanych w zakresie zagospodarowania przestrzennego.

* 1. FOGR – ewidencja decyzji wyłączających grunty z produkcji rolnej - lub równoważny, oferujący integracje z użytkowanym przez zamawiającego systemem STRATEG. Współpracuje z systemami użytkowanymi w wydziale geodezji co mocno usprawni procesy w wydziale architektury:

- rejestracja decyzji wyłączających grunty z produkcji rolnej,

- edycja decyzji i pism związanych z wyłączeniem gruntów z produkcji,

- naliczanie opłat związanych wartością tony zboża w danym roku,

- roczne przeliczanie opłat,

- wykonywanie zestawień zbiorczych (przypisów).

* 1. Połączenie z bazami programu EWMAPA umożliwiające graficzną rejestrację obszarów wyłączonych,
	2. Połączenie z obiektem graficznym decyzji wyłączającej (interfejs pytający i zwrotny do baz programu EWMAPA).

1. Produkty powinny być nowe, wyprodukowane w roku 2022, zapakowane przez producenta, dopuszczone do sprzedaży na terenie Polski.