|  |  |
| --- | --- |
|  | Cyfrowe Mazury  Szczegółowy Opis Przedmiotu Zamówienia:  „Dostawa oprogramowania portalu E-usług oraz oprogramowania szyny danych i zestawu konektorów do integracji portalu z systemem EZD PUW wraz z usługą hostingu, dostawa usługi bezpieczeństwa sieciowego, dostawa sprzętu i wyposażenia komputerowego serwerowego i sieciowego, dostawa punktów publicznego dostępu do sieci internet, usługa modernizacji sieci LAN, usługa szkolenia w zakresie obsługi portalu, świadczenie usługi wsparcia i serwisu” |

Zatwierdził:

………………………………………..…………………….

Mikołajki, 6 października 2017 r.

Spis treści

[2 Wstęp 4](#_Toc498974385)

[2.1 Zarys rozwiązania 4](#_Toc498974386)

[2.2 Słownik pojęć 7](#_Toc498974387)

[3 Określenie Przedmiotu Zamówienia 12](#_Toc498974388)

[4 Wymagania prawne 14](#_Toc498974389)

[5 Wymagania ogólne dotyczące dostarczanego rozwiązania 16](#_Toc498974390)

[6 Zakres 1. Dostawa, instalacja i konfiguracja sprzętu niezbędnego do budowy / przebudowy i ujednolicenia sieci lokalnych w tym serwerów i macierzy oraz stanowisk pracy. Budowa / modernizacja sieci LAN. Instalacja, konfiguracja i uruchomienie publicznych punktów dostępowych WiFi 17](#_Toc498974391)

[6.1 Dostawa sprzętu 17](#_Toc498974392)

[6.1.1 Wymagania ogólne dot. dostarczanego sprzętu 17](#_Toc498974393)

[6.1.2 Wymagania minimalne dotyczące routera CE 18](#_Toc498974394)

[6.1.3 Wymagania minimalne dotyczące serwera– wariant I 21](#_Toc498974395)

[6.1.4 Wymagania minimalne dotyczące serwera – wariant II 23](#_Toc498974396)

[6.1.5 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych 24](#_Toc498974397)

[6.1.6 Stanowiska robocze 27](#_Toc498974398)

[6.1.7 Wymagania minimalne dotyczące przełączników sieciowych 31](#_Toc498974399)

[6.1.8 Wymagania minimalne dotyczące oprogramowania do wirtualizacji serwerów lokalnych 33](#_Toc498974400)

[6.2 Modernizacja sieci LAN 37](#_Toc498974401)

[6.2.1 Informacje ogólne 37](#_Toc498974402)

[6.2.2 Przewidywany zakres prac 38](#_Toc498974403)

[6.2.3 Zakres usług utrzymania sieci LAN w JST 38](#_Toc498974404)

[6.3 Instalacja, konfiguracja i uruchomienie publicznych punktów dostępowych WiFi 39](#_Toc498974405)

[6.3.1 Informacje ogólne 39](#_Toc498974406)

[6.3.2 Miejsce instalacji punktów 39](#_Toc498974407)

[6.3.3 Wymagania minimalne punktów dostępowych 40](#_Toc498974408)

[7 Zakres 2. Dostawa Systemów EOD, Szyn Danych lokalnych i centralnej wraz z zestawem konektorów oraz Portalu Usług Elektronicznych 43](#_Toc498974409)

[7.1 System EOD (EZD PUW) 43](#_Toc498974410)

[7.2 Usługi udostępnione dla poziomu centralnego 43](#_Toc498974411)

[7.3 Wdrożenie EOD, integracji 43](#_Toc498974412)

[8 Zakres 3. Dostarczenie i wdrożenie formularzy elektronicznych 45](#_Toc498974413)

[9 Zakres 4. Wdrożenie Portalu Usług Elektronicznych i centralnej Szyny Danych oraz zapewnienie bezpieczeństwa transmisji danych. 48](#_Toc498974414)

[9.1 Warstwa administracji i integracji 48](#_Toc498974415)

[9.2 Moduł konta klienta 52](#_Toc498974416)

[9.3 Moduł elektronicznego biura interesanta 53](#_Toc498974417)

[9.4 Moduł płatności online 54](#_Toc498974418)

[9.5 Warstwa Szyny Danych 57](#_Toc498974419)

[9.6 Zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy 58](#_Toc498974420)

[9.7 Integracja SUE z Lokalnymi Szynami Danych 75](#_Toc498974421)

[9.8 Wdrożenie 75](#_Toc498974422)

[10 Zakres 5. Przygotowanie i przeprowadzenie pakietów szkoleń. 77](#_Toc498974423)

[11 Zakres 6. Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej. 78](#_Toc498974424)

[12 Zakres 7. Świadczenie usługi serwisu 79](#_Toc498974425)

[13 Zastrzeżenie równoważności rozwiązań 81](#_Toc498974426)

[14 Spis tabel: 82](#_Toc498974427)

# Wstęp

Niniejszy dokument stanowi Szczegółowy Opis Przedmiotu Zamówienia (OPZ) w zakresie dostawy i wdrożenia oprogramowania (obiegu dokumentów, integracji z systemami dziedzinowymi oraz portalu eUsług) oraz sprzętu i usług bezpieczeństwa w projekcie „Cyfrowe Mazury”.

## Zarys rozwiązania

Rozwiązanie informatyczne wraz z usługą wdrożenia, integracji i gwarancji stanowi rozwiązanie dostarczane dla Partnerów projektu ze Stowarzyszenia Wielkie Jeziora Mazurskie 2020. Rozwiązanie ma na celu podniesienie dostępności usług świadczonych drogą elektroniczną na terenie Wielkich Jezior Mazurskich.

W skład Partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020 wchodzą podmioty:

1. Gmina Miasto Giżycko - 11-500 Giżycko, Al. 1 Maja 14
2. Gmina Giżycko - 11-500 Giżycko, ul. Mickiewicza 33
3. Gmina Miłki - 11-513 Miłki, ul. Mazurska 2
4. Gmina Orzysz - 12-250 Orzysz, ul. Giżycka 15
5. Gmina Ruciane Nida - 12-220 Ruciane-Nida, Aleja Wczasów 4
6. Gmina Mikołajki - 11-730 Mikołajki, ul. Kolejowa 7
7. Gmina Miasto Mrągowo - 11-700 Mrągowo, ul. Królewiecka 60A
8. Gmina Mrągowo - 11-700 Mrągowo, ul. Królewiecka 60A
9. Gmina Ryn – 11-520 Ryn, ul. Świerczewskiego 2
10. Gmina Pozezdrze - 11-610 Pozezdrze, al. 1 Maja 1a
11. Powiat Giżycki –**dwa budynki**:

* al. 1 Maja 14, 11-500 Giżycko
* ul. Generała Józefa Zajączka 2, 11-500 Giżycko

1. Gmina Węgorzewo - 11-600 Węgorzewo, ul. Zamkowa 3

Dostępność usług elektronicznych w tym regionie jest niewystarczająca, w tym celu Zamawiający określił przedmiot zamówienia precyzując zadania, jakie Wykonawca musi zrealizować w ramach projektu.

Na poziomie lokalnym, tj. u każdego z Partnerów projektu zostanie dostarczony i wdrożony system Elektronicznego Obiegu Dokumentów wraz z Szyną Danych lub zestawem konektorów. Wykonawca dostarczy integrację rozwiązania Elektronicznego Obiegu Dokumentów z System Dziedzinowym Partnera poprzez Szynę Danych lokalną/dedykowane konektory programowe.

U każdego z partnerów nastąpi ujednolicenie architektury sieci lokalnej, w skład której wejdą:

* serwer - kontroler domeny,
* serwer aplikacji EZD zawierający przestrzeń dyskową na lokalny skład dokumentów bieżących,
* serwer poczty e-mail,
* skanery – minimum dwie sztuki. Możliwe są skanery dwóch typów: „duży” – skaner A4 wysokoprzebiegowy; „mały” – szybki skaner A4,
* przełączniki sieciowe,
* router CE umożliwiający dostęp poprzez wspólny dla wszystkich JST w projekcie protokół (MPLS) oraz udostępniający wybrane funkcje zarządzania dostępem do sieci LAN,
* mechanizm zapewnienia backupu i archiwizacji danych partnerów,
* sieci lokalne LAN zostaną zmodernizowane do min. kategorii 5e; wszelkie prace instalacyjne związane z rozbudową sieci LAN zostaną wykonane zgodnie ze schematami zamieszczonymi w Załączniku nr 9 do SIWZ oraz w porozumieniu z lokalnymi administratorami sieci, ilość punktów elektryczno-logicznych zostanie zwiększona zgodnie z poniższą tabelą:

Tabela 1. Ramowy wykaz ilości minimalnych dostarczanych rozwiązań do poszczególnych Partnerów Projektu

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nazwa jednostki** | Starostwo Powiatowe w Giżycku - 2 lokalizacje | Urząd Gminy w Giżycku | Urząd Miejski w Giżycku | Urząd Miejski w Mrągowie | Urząd Miejski w Węgorzewie | Urząd Miasta i Gminy Ruciane-Nida | Urząd Miasta i Gminy Mikołajki | Urząd Miasta i Gminy Ryn | Urząd Miejski w Orzyszu | Urząd Gminy Miłki | Urząd Gminy Pozezdrze | Urząd Gminy Mrągowo |
| Stacje do centrum zarządzania/monitorowania wdrożonych systemów i sprzętu | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| Oprogramowanie zarządzające i monitorujące VM | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Serwery [z usługami: Microsoft Windows Serwer / Active Directory / EZD, itd.] | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Motor bazy danych Microsoft®SQL Express / lub równoważny funkcjonalnie kompatybilny z systemem EOD | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Oprogramowanie serwera poczty e-mail | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Skaner - mały | 1 | 1 | 1 | 2 | 1 | 1 | 5 | 1 | 3 | 1 | 1 | 2 |
| Skaner - duży | 1 | 1 | 1 | 2 | 1 | 1 | 3 | 1 | 2 | 1 | 1 | 1 |
| Czytniki kodów kreskowych | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Drukarki etykiet | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Zestaw punktów dostępowych PublicWiFi [1 zestaw = 10 AP] | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| Stanowisko robocze - laptop | 2 | 1 | 2 | 0 | 0 | 0 | 5 | 2 | 5 | 3 | 4 | 0 |
| Przełącznik 48 port | 2 | 2 | 2 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 2 |
| Stanowisko robocze - komputer stacjonarny | 8 | 20 | 18 | 28 | 0 | 27 | 10 | 12 | 33 | 17 | 15 | 14 |
| Sieć elektryczno-logiczna (liczba PEL do naprawy lub instalacji) | 61 | 40 | 0 | 0 | 0 | 60 | 0 | 30 | 0 | 26 | 0 | 0 |

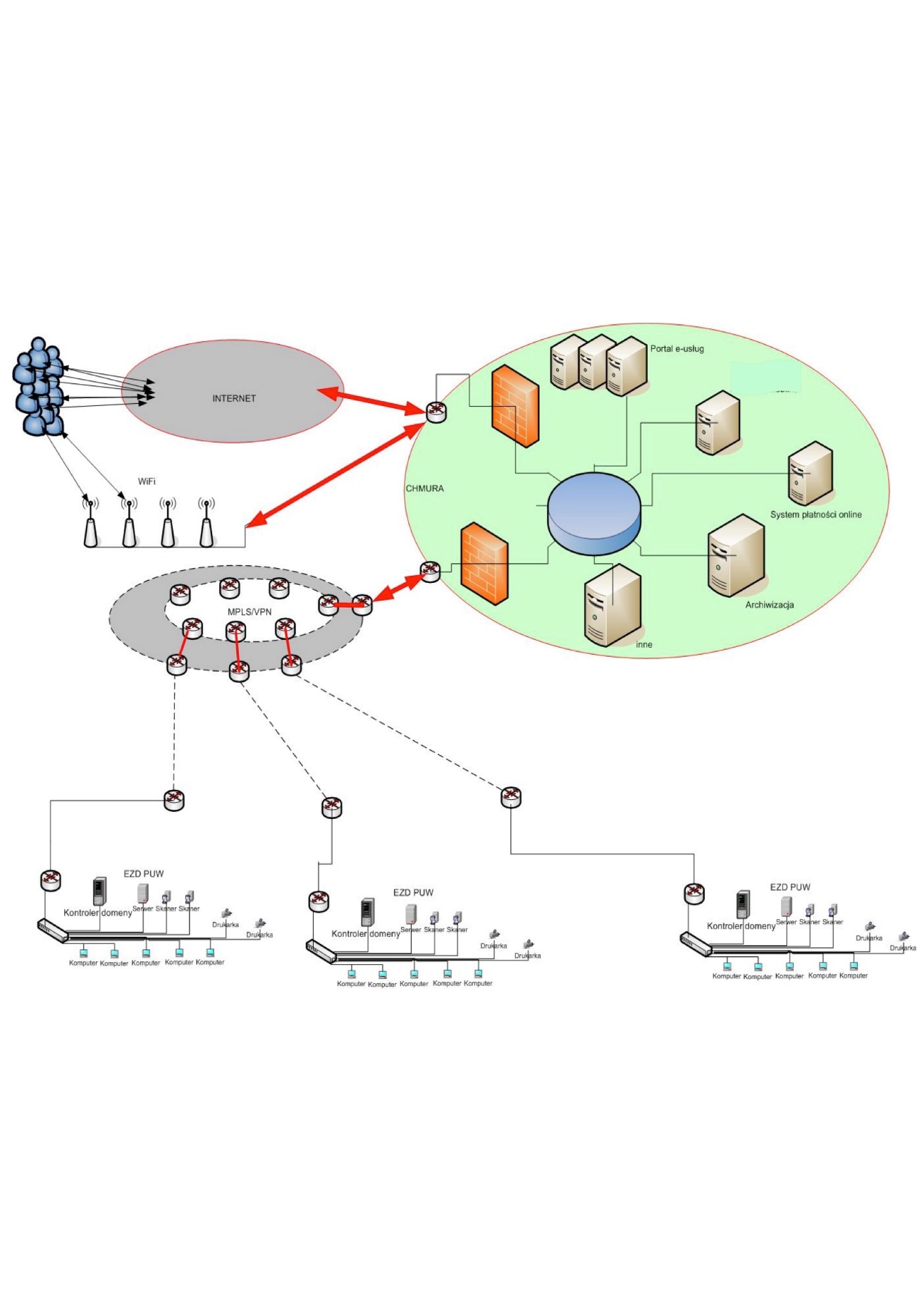
Wszystkie zapisy dotyczące ilości serwerów w znaczeniu usług, nie oznaczają maszyn fizycznych a jedynie maszyny logiczne. Dopuszczalne zatem jest instalowanie więcej niż jednej maszyny logicznej na jednej maszynie fizycznej przy zachowaniu wysokiej dostępności usług [HA].

Zastosowanie protokołu szyfrowanego MPLS umożliwi stworzenie zarządzanego wspólnego medium dostępowego partnerów do platformy udostępnionej w chmurze obliczeniowej (IAAS). Dla wszystkich routerów brzegowych zostanie opracowany wspólny plan adresacji zapewniający możliwość dodawania nowych JST oraz dostęp pracowników utworzonego na potrzeby projektu centrum kompetencji do zasobów teleinformatycznych każdego JST.

Zadaniem Centrum Kompetencji będzie świadczenia usługi 2 linii wsparcia w zakresie utrzymania LAN i aplikacji dziedzinowych wszystkich uczestników projektu.

Na poziomie centralnym zostanie dostarczona usługa chmury IAAS, na której umieszczone zostaną: Portal Usług Elektronicznych, Formularze elektroniczne oraz Szyna Danych centralna wraz z zestawem dedykowanych konektorów programowych. Portal Usług Elektronicznych będzie stanowił jeden punkt dostępowy do Cyfrowego Urzędu każdego z partnerów i będzie zintegrowany za pomocą centralnej szyny danych z jednostkami samorządowymi na poziomie lokalnym. Dostęp do chmury realizowany będzie przez operatora chmury, który dostarczy każdemu partnerowi usługę polegającą na dostarczeniu łącza do transmisji danych z dostępem do chmury; w niej do zasobów o określonej wydajności i z przestrzenią dyskową; określonym w umowie poziomem bezpieczeństwa oraz dostępem do Internetu. W ramach usługi zapewniany będzie także serwis o określonym poziomie jakościowym (SLA).

Idea całości rozwiązania przedstawiona jest na rysunku poniżej :



Rysunek 1 Schemat ideowy zamawianego rozwiązania.

## Słownik pojęć

Na potrzeby niniejszego postępowania stosuje się następujące pojęcia i definicje:

1. **Strony Umowy** – uogólnione pojęcie stosowane zamiennie do określenia Zamawiającego i Wykonawcy jednocześnie.
2. **Cel Umowy** – przyczyny oraz oczekiwane wyniki, dla osiągnięcia których Strony podjęły współpracę i zawarły Umowę.
3. **Przedmiot Umowy** – całokształt zagadnień realizowanych w ramach Umowy ukierunkowanych na osiągnięcie Celu Umowy.
4. **Dysfunkcja** – zbiorcze określenie dla nieprawidłowości rozumianych jako niezgodność z Dokumentacją lub też uciążliwość w pracy z Systemem.
5. **Kategoria Dysfunkcji** - kategoria, do której kwalifikowane jest Zgłoszenie Serwisowe dotyczące Dysfunkcji. Wyróżniamy następujące Kategorie wg kryteriów:
   * + - 1. **Stan Krytyczny** – dysfunkcja Systemu, która prowadzi do zatrzymania eksploatacji systemu, utraty danych lub naruszenia ich spójności, w wyniku którego niemożliwe jest prowadzenie bieżącej działalności przy użyciu Systemu.
         2. **Awaria** – oznacza dysfunkcję Systemu, uniemożliwiającą prawidłowe użytkowanie Systemu lub jego części, jednak nie prowadzi do zatrzymania eksploatacji Systemu.
         3. **Błąd** – powtarzalne działanie Systemu niezgodne z jego dokumentacją użytkową, uniemożliwiające wykonanie części jego funkcji.
         4. **Usterka** - zakłócenie działania oprogramowania, polegające na nienależytym działaniu jego części, nie ograniczające działania całego systemu; nie mające istotnego wpływu na zastosowanie oprogramowania i nie będące awarią lub błędem.
6. **Prace Serwisowe** - działania Wykonawcy mające na celu realizację Zgłoszenia Serwisowego.
7. **Naprawa** – modyfikacja Systemu usuwająca Dysfunkcję Systemu.
8. **Obejście** - tymczasowe rozwiązanie pozwalające na prawidłowe wykorzystanie oprogramowania bez usuwania wykrytego błędu przy zachowaniu integralności bazy danych.
9. **Realizacja Zgłoszenia Serwisowego** - zakończenie Prac Serwisowych, w wyniku których przywrócono Stan Funkcjonalności.
10. **Analiza** – dokumenty opracowane przez Wykonawcę, mające na celu doprecyzowanie sposobu realizacji wymagań Zamawiającego, zasad i metod realizacji Umowy oraz wskazanie i szczegółowe opisanie Produktów;
11. **Backup** – wykonanie kopii bezpieczeństwa danych pozwalających na odtworzenie i przywrócenie Bazy Danych i Systemu po wystąpieniu awarii w przypadku utraty lub uszkodzenia oryginalnych danych; jakość odtworzonych danych powinna być dostosowana do ustalonego uprzednio poziomu ryzyka, który poniesie Zamawiający (poziom ryzyka determinuje cykliczność wykonywania backup'ów).
12. **Baza Danych** – zbiór wszystkich danych zewidencjonowanych za pomocą Systemu.
13. **Czas Roboczy** – czas pracy liczony w Dni Robocze, w którym świadczona jest pomoc telefoniczna przy eksploatacji Systemu.
14. **Dzień Roboczy** – dzień kalendarzowy od poniedziałku do piątku z wyłączeniem świąt i dni ustawowo wolnych od pracy.
15. **Dokumentacja** – dokument papierowy lub elektroniczny opisujący System i zasady użytkowania Systemu. Wszelka dokumentacja sporządzona przez Wykonawcę dostarczona i modyfikowana w wyniku realizacji umowy.
16. **Godziny robocze** – czas pracy liczony w Dni Robocze w godzinach 7:30 – 15:30.
17. **Konsultant serwisowy** – osoba fizyczna posiadająca odpowiednie kwalifikacje uprawniające do realizowania Serwisu.
18. **Pomoc Telefoniczna** – świadczenie konsultacji telefonicznej dotyczące szeroko pojętej eksploatacji Systemu.
19. **Procedura** – schemat postępowania w jaki winien być realizowany określony fragment Przedmiotu Umowy.
20. **Publikacja** – udostępnienie Systemu zawierającego zmienioną funkcjonalność.
21. **Serwer** – sprzęt komputerowy, na którym zainstalowana jest baza danych wykorzystywana przez System.
22. **Serwis** – usługa o charakterze technicznym, organizacyjnym, doradczym i szkoleniowym, przeznaczona do zapewnienia stabilnej pracy Systemu.
23. **Stan Funkcjonalności** - stan Systemu, w którym nie występują Dysfunkcje.
24. **Upgrade** – nowa  wersja Systemu związana ze stworzeniem nowej funkcjonalności.
25. **Update** – aktualizacja Systemu w wyniku zmian przepisów, związanych bezpośrednio i pośrednio z systemem ochrony zdrowia, w zakresie tej samej wersji Systemu.
26. **Wdrożenie** – opisane Umową świadczenia Wykonawcy mające na celu wykonanie Systemu
27. **Wersja** – okresowa Publikacja Systemu uwzględniająca Naprawy i zmiany dokonane w okresie od poprzedniej Publikacji Systemu. Wydanie Wersji obejmuje również opis nowej Funkcjonalności Systemu.
28. **Wydanie Systemu** – okresowa Publikacja Systemu obejmująca nową funkcjonalność Systemu oraz nową Dokumentację.
29. **Zgłoszenie Serwisowe** – Dysfunkcja, o której Wykonawca został powiadomiony drogą mailową.
30. **Administrator** - Użytkownik konfigurujący i zarządzający Systemem i Infrastrukturą.
31. **API** - Application Programming Interface, interfejs programowania aplikacji – jest to sposób rozumiany, jako ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.
32. **Architektura systemu teleinformatycznego** – opis składników systemu teleinformatycznego, powiązań i relacji pomiędzy tymi składnikami.
33. **Czas dostarczenia rozwiązania** - Okres czasu od wysłania Zgłoszenia do usunięcia przyczyny problemu lub zastosowania Rozwiązania Zastępczego.
34. **Dane typu on-line** – dane dostępne w czasie rzeczywistym tzn. natychmiast po wprowadzaniu do określonego modułu systemu.
35. **Dane typu off-line** – dane pochodzące z migracji z innych modułów systemu lub zarchiwizowane, dostępne w czasie zdefiniowanym przez administratora systemu.
36. **Dane referencyjne** - dane opisujące cechę informacyjną obiektu pierwotnie wprowadzone do rejestru publicznego w wyniku określonego zdarzenia, z domniemania opatrzone atrybutem autentyczności .
37. **Dokument Elektroniczny (DE)** - Dokument Elektroniczny w rozumieniu przepisów Art. 3 ust. 2) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005r. Nr 64, poz. 565 z późn. zm.).
38. **Dostępność** – właściwość określająca, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w założonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym .
39. **ePUAP** – Elektroniczna Platforma Usług Administracji Publicznej https://epuap.gov.pl
40. **ESB, szyna usług, szyna ESB** (ang. Enterprise Service Bus) - oparte na otwartych standardach oprogramowanie typu, „middleware”, które dostarcza możliwość bezpiecznego współdziałania (interoperacyjność) aplikacji poprzez interfejsy usług sieciowych (web services). Szyna usługowa zapewnia wymianę informacji pomiędzy aplikacjami opartymi na różnych technologiach, działających na różnych platformach poprzez usługi integracyjne takie jak transformacje i inteligentny routing informacji. Dzięki zastosowaniu takiego rozwiązania usługi mogą być dowolnie konfigurowane, rozszerzane, przemieszczane lub podmieniane bez przerywania pracy systemów biznesowych lub modyfikowania aplikacji.
41. **ESP** – Elektroniczna Skrzynka Podawcza
42. **EZD, EOD** - Elektroniczne Zarządzanie Dokumentacją, oprogramowanie dedykowane do wykonywania ewidencji czynności kancelaryjnych w JST w rozumieniu przepisów Instrukcji Kancelaryjnych. Oprogramowanie to realizuje funkcje rejestracji, przechowywania dokumentów w wersji elektronicznej w repozytoriach oraz ewidencjonowania obiegu korespondencji i spraw w obrębie JST
43. **EZD PUW** – System EZD autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku (https://ezd.gov.pl)
44. **Formularz Elektroniczny** - Graficzny interfejs użytkownika wystawiany przez oprogramowanie służący do przygotowania wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego w rozumieniu przepisów rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2011, Nr206, poz.1216).
45. **Integralność** – właściwość polegająca na tym, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony .
46. **IAAS** – chmura obliczeniowa udostępniająca Zamawiającemu zasoby infrastruktury serwerów oraz infrastruktury bezpieczeństwa dostępu do sieci.
47. **JST** – Jednostka Samorządu Terytorialnego
48. **Kierownik Projektu Wykonawcy** (KPW) – Osoba ze strony Wykonawcy upoważniona do bezpośredniej koordynacji zadań objętych umową. Do zadań Kierownika Projektu Wykonawcy należy m.in. podpisywanie dokumentów w zakresie Protokołów Odbioru Zadań, Protokołów Odbioru Końcowego.
49. **Kierownik Projektu Zamawiającego** (KPZ) - Osoba ze strony Zamawiającego upoważniona do bezpośredniej koordynacji zadań objętych umową. Do zadań Kierownika Projektu Zamawiającego należy m.in. podpisywanie dokumentów w zakresie Protokołów Odbioru Zadań, Protokołów Odbioru Końcowego.
50. **KPA** – Kodeks Postepowania Administracyjnego
51. **Moduł systemu** – kompletny zestaw narzędzi informatycznych obejmujących wszystkie warstwy architektury systemu, który dostarcza aplikację przeznaczoną dla użytkownika końcowego do realizacji określonych dziedzin działalności Zamawiającego.
52. **Okno Serwisowe** – przerwa w działaniu systemu w godzinach pracy [tj. pomiędzy 7:30 a 15:30] w dni robocze Zamawiającego, mająca na celu umożliwienie prowadzenie prac serwisowych wymagających czasowego wyłączenia systemu [np. aktualizacja]. Poza tymi godzinami aktywny 365/24/7 system HelpDesk. Okno serwisowe dotyczy usług serwisowych z wyłączeniem zadań bezpieczeństwa sieci.
53. **Oprogramowanie aplikacyjne** – System Dziedzinowy (SD), Elektroniczne Zarządzanie Dokumentacją (EZD), System usług elektronicznych dla mieszkańców (SUE) oraz oprogramowanie integrujące.
54. **Oprogramowanie standardowe** – Każde oprogramowanie niezbędne, poza oprogramowaniem aplikacyjnym niezbędne do działania Systemu.
55. **Pakiet Usług Elektronicznych** – lista dostarczonych formularzy elektronicznych wraz ze wzorami dokumentów elektronicznych dla Zamawiającego
56. **Portal Usług Elektronicznych** – portal umiejscowiony w chmurze IAAS udostępniający usługi elektroniczne dostarczane przez System dla użytkowników wewnętrznych i zewnętrznych
57. **PKI** – Infrastruktura Klucza Publicznego
58. **PZ ePUAP** – Profil Zaufany ePUAP
59. **Rozwiązanie zastępcze** - proponowane przez Wykonawcę rozwiązanie tymczasowe, usuwające lub niwelujące czasowo do akceptowalnego poziomu skutki wystąpienia Wady, wprowadzone do czasu usunięcia Wady.
60. **SRP System Rejestrów Państwowych** - Projekt realizowany przez Centralny Ośrodek Informatyki dla MSW udostępnia aplikację Źródło, ułatwiającą korzystanie z SRP. Program obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych i stanu cywilnego.
61. **System** – Łączne określenie dla oprogramowania – występującego u Zamawiającego, objętego wdrożeniem oraz umową serwisową z Wykonawcą, bez względu na nazwę handlową. Obejmujący Platformę systemowo-sprzętową, Oprogramowania aplikacyjne oraz inne oprogramowanie niezbędne do działania SD, EZD i SUE realizowanego w niniejszym zamówieniu.
62. **System Dziedzinowy** (SD) - Oferowany przez Wykonawcę zintegrowany system informatyczny dedykowany do obsługi działalności JST.
63. **SUE System Usług Elektronicznych** – system do publikowania i zarządzania usługami elektronicznymi udostępnionymi dla klientów JST w postaci portalu www.
64. **System zewnętrzny** - Każdy System informatyczny niebędący przedmiotem Zamówienia a oddziaływujący na przedmiot zamówienia.
65. **Usługi elektroniczne (eUsługi)** – usługi, których świadczenie odbywa się za pomocą Internetu, jest zautomatyzowane (może wymagać niewielkiego udziału człowieka) i zdalne. Od usługi w ujęciu tradycyjnym, eUsługę odróżnia brak udziału człowieka po drugiej stronie oraz świadczenie na odległość.
66. **Użytkownik** - Osoba, która jest pracownikiem Zamawiającego, posiada swój unikalny login i hasło i wykonuje za pomocą EZD lub SD lub SUE obowiązki służbowe.
67. **Web Service** - Usługa sieciowa dostarczająca określoną funkcjonalność poprzez sieci Internet, niezależnie od platformy sprzętowej i implementacji.
68. **Wzór dokumentu elektronicznego** - Wzór pisma w formie Dokumentu Elektronicznego w rozumieniu Art.19 b) ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005r. Nr 64 z późn. zm.) oraz §18 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 roku w sprawie sporządzania pism w postaci dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych. (Dz.U. z 2011, Nr206, poz.1216).
69. **Wykonawca** – wybrany w drodze zamówienia publicznego podmiot realizujący niniejszy przedmiot zamówienia.
70. **Zamawiający** – Stowarzyszenie Wielkie Jeziora Mazurskie 2020
71. **Zdalny dostęp** – możliwość realizacji usług wsparcia, wdrożenia i gwarancji związanych z systemem z dowolnego miejsca za pośrednictwem bezpiecznego połączenia internetowego.
72. **XML** – Format XML jest to obecnie powszechnie uznany standard publiczny, umożliwiający wymianę danych między różnymi systemami.

# Określenie Przedmiotu Zamówienia

Zamówienie dotyczy następujących jednostek samorządowych:

Tabela 2 Wykaz lokalizacji partnerów biorących udział w Projekcie

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.Starostwo Powiatowe w Giżycku (dwa oddzielne budynki) | 2.Urząd Gminy w Giżycku | 3.Urząd Miejski w Giżycku | 4.Urząd Miejski w Mrągowie | 5.Urząd Miejski w Węgorzewie | 6.Urząd Miasta i Gminy Ruciane-Nida | 7.Urząd Miasta i Gminy Mikołajki | 8.Urząd Miasta i Gminy Ryn | 9.Urząd Miejski w Orzyszu | 10.Urząd Gminy Miłki | 11.Urząd Gminy Pozezdrze | 12.Urząd Gminy Mrągowo |
| **Giżycko** | **Giżycko** | **Giżycko** | **Mrągowo** | **Węgorzewo** | **Ruciane-Nida** | **Mikołajki** | **Ryn** | **Orzysz** | **Miłki** | **Pozezdrze** | **Mrągowo** |
| Lokalizacja **1** | Lokalizacja **2** | Lokalizacja **3** | Lokalizacja **4** | Lokalizacja **5** | Lokalizacja **6** | Lokalizacja **7** | Lokalizacja **8** | Lokalizacja **9** | Lokalizacja **10** | Lokalizacja **11** | Lokalizacja **12** |

Przedmiotem Zamówienia podzielony jest na następujące zakresy składowe:

Tabela 3 Ramowe zestawienie zakresu przedmiotu zamówienia

|  |  |  |
| --- | --- | --- |
| Lp. | Opis prac wykonanych w ramach zakresu | Czas realizacji |
| Zakres 1 | Dostawa, instalacja i konfiguracja sprzętu niezbędnego do budowy / przebudowy i ujednolicenia sieci lokalnych w tym serwerów i macierzy oraz stanowisk pracy. Budowa / modernizacja sieci LAN. Instalacja, konfiguracja i uruchomienie publicznych punktów dostępowych WiFi. | 4 miesiące |
| Zakres 2 | Dostawa portalu Usług elektronicznych oraz integracja z Szyną Danych na poziomie lokalnym. | 6 miesięcy |
| Zakres 3 | Dostarczenie i wdrożenie formularzy elektronicznych dla każdego z partnerów projektu | 6 miesięcy |
| Zakres 4 | Wdrożenie portalu Usług elektronicznych i Szyny Usług wraz z integracją na poziomie centralnym oraz integracją z poziomami lokalnymi w tym zapewnienie bezpieczeństwa transmisji danych oraz dostępu do PUE za pomocą dedykowanych łączy o przepustowości nie mniejszej niż 100 Mbps (symetrycznej). | 6 miesięcy |
| Zakres 5 | Przygotowanie i przeprowadzenie szkoleń w zakresie użytkowania i administrowania e-usługami. | 6 miesięcy |
| Zakres 6 | Przygotowanie i dostarczenie dokumentacji projektowej i powykonawczej | 2 miesiące |
| Zakres 7 | Świadczenie następujących usług wsparcia w ramach dostarczonego rozwiązania:  - 3 linii wsparcia dla wszystkich partnerów projektu;  - serwisu dostarczonego/wytworzonego oprogramowania;  - utrzymania w pełnym zakresie IAAS w lokalizacji głównej;  - utrzymanie łączy dostępowych z lokalizacji terenowych partnerów do lokalizacji głównej oraz dostępu do sieci Internet z lokalizacji głównej; | 60 miesięcy**[[1]](#footnote-1)** |

Szczegółowy opis produktów i zakresów prac określono w kolejnych rozdziałach dokumentu.

# Wymagania prawne

Oferowane przez Wykonawcę rozwiązania muszą być na dzień odbioru zgodne z wszystkimi obowiązującymi Zamawiającego aktami prawnymi regulującymi pracę urzędów administracji publicznej oraz usług urzędowych realizowanych drogą elektroniczną. Oferowane rozwiązania muszą być zgodne w szczególności z następującymi przepisami:

1. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (t. j. Dz. U. 2011 r. Nr 14 poz. 67 z późn. zm.).
2. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t. j. Dz. U. 2013 r. poz. 267).
3. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t. j. Dz. U. 2011 r. Nr 123 poz. 692 z późn. zm.).
4. Rozporządzenie Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych (Dz. U. 2002 r. Nr 167 poz. 1375)
5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. 2006 r. Nr 206 poz. 1517).
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz. U. 2006 r. Nr 206 poz. 1518).
7. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych (Dz. U. 2006 r. Nr 206 poz. 1519).
8. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. 2002 r. Nr 101 poz. 926 z późn. zm.).
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim muszą odpowiadać urządzenia i Systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 2004 r. Nr 100 poz. 1024).
10. Ustawa z dnia 22 stycznia 1999 o ochronie informacji niejawnych (t. j. Dz. U. 2005 r. Nr 196 poz. 1631 z późn. zm.)
11. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2001 r. Nr 112 poz. 1198 z późn. zm.).
12. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. 2007 r. Nr 10 poz. 68).
13. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (t. j. Dz. U. 2013 r. poz.262).
14. Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. 2002 r. Nr 128 poz. 1094).
15. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2013 r. poz. 1422).
16. Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. 2013 r. poz.235).
17. Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. 2005 r. Nr 205 poz. 1692).
18. Ustawa z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. 2014 poz. 183).
19. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 12 kwietnia 2012 r. (Dz.U. z 2012 r., poz. 526)
20. Rozporządzenie Prezesa Rady Ministrów w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych z dnia 14 września 2011 r. (Dz.U. Nr 206, poz. 1216)
21. Rozporządzenie Ministra Administracji i Cyfryzacji w sprawie wzoru i sposobu prowadzenia metryki sprawy z dnia 6 marca 2012 r. (Dz.U. z 2012 r. poz. 250). lub innymi, które zastąpią ww. w dniu wdrożenia rozwiązania.

# Wymagania ogólne dotyczące dostarczanego rozwiązania

Tabela 4 Wymagania ogólne dotyczące dostarczanego rozwiązania

|  |  |
| --- | --- |
| KOD | Wymaganie |
| WP1 | System musi być zbudowany i wdrożony zgodnie z obowiązującymi przepisami prawa, zgodnie z strukturą organizacyjną i regulaminem urzędu oraz dobrymi praktykami funkcjonującymi w JST |
| WP2 | Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień jego instalacji (tzn. powinno być dostosowane do zmieniających się powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Zamawiającego). |
| WP3 | System musi umożliwiać definiowanie dowolnej ilości użytkowników. Zamawiający dopuszcza ograniczenia dot. ilości użytkowników serwera poczty e-mail, do minimum 1000 skrzynek/serwer. |
| WP4 | System musi być w całości spolonizowany, a więc posiadać polskie znaki i instrukcję obsługi po polsku dla użytkownika oraz administratora. Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, punkty wifi, itp. dla których wymogiem minimalnym jest posiadanie interfejsów w języku minimum angielskim. Zamawiający, dopuszcza nie w pełni spolonizowane oprogramowanie w zakresie: oprogramowania wbudowanego, np. firmware kart rozszerzeń, poleceń CLI, BIOS, UEFI, IDRAC, IPMI, iLO, itp.., oraz specjalistycznych narzędzi diagnostycznych i zarządzania dedykowanymi dla działów IT oraz narzędzi do wirtualizacji. |
| WP5 | System musi posiadać graficzny interfejs użytkownika gwarantujący wygodne wprowadzanie danych, przejrzystość prezentowania danych na ekranie oraz wygodny sposób wyszukiwania danych po dowolnych kryteriach. Wyjątek stanowią urządzenia wysoko specjalistyczne np. routery, przełączniki, serwery, macierze, punkty wifi, itp. dla których wymogi minimalne co do posiadanych interfejsów zostały opisane odrębnie. |
| WP6 | System musi gwarantować integralność danych, bieżącą kontrolę poprawności wprowadzanych danych, spójność danych. |
| WP7 | System musi pracować w środowisku sieciowym i posiadać wielodostępność pozwalającą na równoczesne korzystanie z bazy danych przez wielu użytkowników bez ograniczeń na ich liczbę. |
| WP8 | System musi gwarantować dostępność przez publiczną sieć Internet Portalu Usług Elektronicznych zintegrowanego z Systemami Dziedzinowymi oraz EZD. |
| WP9 | System musi posiadać mechanizmy umożliwiające weryfikację integralności danych tj. identyfikację użytkownika i ustalenie daty wprowadzenia i modyfikacji danych. |
| WP10 | System musi posiadać mechanizmy ochrony danych przed niepowołanym dostępem, nadawania uprawnień dla użytkowników do korzystania z modułów jak również do korzystania z wybranych funkcji. |
| WP11 | System musi posiadać modyfikowalne słowniki wewnętrzne. |
| WP12 | System musi działać w środowisku zintegrowanych baz danych posiadającym następujące cechy: relacyjność i transakcyjność, komunikacja z aplikacjami w standardzie SQL. |
| WP13 | Na dzień składania oferty dostarczany w ramach Projektu System nie może być przeznaczony do wycofania z produkcji, sprzedaży lub wsparcia technicznego. |
| WP14 | Dostarczone oprogramowanie musi być oprogramowaniem w wersji aktualnej. |
| WP15 | Dla dostarczonego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne, instrukcje użytkownika i administratora (w formie elektronicznej). |
| WP16 | System powinien być zintegrowany pod względem przepływu informacji - informacja raz wprowadzona do systemu jest wykorzystywana w pozostałych modułach programowych. |
| WP17 | Dla dostarczonego oprogramowania należy dostarczyć: bezterminowe licencje użytkowe oraz subskrypcyjne, okresowe [np. na aktualizację sygnatur wirusów] na min. okres trwałości projektu, tj. 60 msc; nośniki instalacyjne. |

# Zakres 1. Dostawa, instalacja i konfiguracja sprzętu niezbędnego do budowy / przebudowy i ujednolicenia sieci lokalnych w tym serwerów i macierzy oraz stanowisk pracy. Budowa / modernizacja sieci LAN. Instalacja, konfiguracja i uruchomienie publicznych punktów dostępowych WiFi

## Dostawa sprzętu

### Wymagania ogólne dot. dostarczanego sprzętu

Tabela 5 Wymagania ogólne dot. dostarczanego sprzętu

|  |  |
| --- | --- |
| Kod | Wymaganie |
| WSZL15 | Router CE – w każdej lokalizacji JST (1 do 12) zainstalowany zostanie router CE. Opis wymagań na urządzenie zawarto w rozdziale 6.1.2 |
| WSZL16 | Serwer - Do lokalizacji 5,6,7,8,9,10,11 (do 50 użytkowników) Wykonawca dostarczy po min. dwa serwery fizyczne spełniające wymagania z rozdziału 6.1.3; do lokalizacji 1,2,3,4,12 (od 51-150 użytkowników) Wykonawca dostarczy po min. dwa serwery fizyczne spełniające wymagania z rozdziału 6.1.4 |
| WSZL17 | Macierze dyskowe w zasobach lokalnych – Wykonawca dostarczy po min. jednej macierzy dyskowej do każdego uczestnika projektu o parametrach minimalnych określonych w rozdziale 6.1.5 |
| WSZL18 | Komputery stacjonarne w zasobach lokalnych – Wykonawca dostarczy komputery , laptopy oraz sprzęt dodatkowy o parametrach minimalnych określonych w rozdziale 6.1.6 |
| WSZL19 | Zamawiający wymaga uruchomienia na serwerach fizycznych maszyn wirtualnych realizujących następujące zadania: Kontroler AD, serwer pocztowy, serwer EZD + innych niezbędnych do pracy całości komponentów [np. DNS, DHCP, NTP] w oparciu o oprogramowanie do wirtualizacji o parametrach minimalnych określonych w rozdziale 6.1.8 |
| WSZL20 | Zamawiający wymaga dostawy przełączników do wszystkich lokalizacji. Parametry minimalne przełączników opisane są w rozdziale 6.1.7. W ramach Systemu Wykonawca musi zapewnić odpowiedni dla płynnej pracy wszystkich modułów Systemu: poziom bezpieczeństwa oraz wydajności połączeń pomiędzy serwerami a macierzami. Wymaga się aby w przyszłości można było dołączyć bez modernizacji sieci LAN [w szczególności przełącznika w serwerowni] dodatkowych serwerów i macierzy z pełną obsługiwaną prędkością. |
| WSZL21 | Zamawiający wymaga aby w lokalizacjach Partnerów Projektu Wykonawca zapewnił zabezpieczenie systemu przed zanikiem napięcia sieciowego o następujących parametrach minimalnych :   * System zapewniający podtrzymanie zasilania dostarczonego rozwiązania przez czas nie krótszy niż 15 min dla całego dostarczonego środowiska sprzętowego – serwery, lub jeśli czas bezpiecznego wyłączenia systemu jest dłuższy niż 15 minut umożliwiający automatyczne i bezpieczne wyłączenie systemu. Z czasem przełączania po zaniku napięcia na wewnętrzne źródło prądu umożliwiającym ciągłą pracę serwerów i macierzy [rzędu 6ms]. * Zostanie zapewnione wsparcie/wymiana elementów wytwarzających i przechowujących energię elektryczną, np. akumulatorów przez okres trwania Projektu * System musi pozwalać na zdalne zarządzanie i monitorowanie, przynajmniej w zakresie alarmów, aktualnego stanu pracy, pozostałego czasu podtrzymania napięcia. * System musi umożliwiać automatyczne powiadamianie określonych osób o wystąpieniu określonych alarmów/zdarzeń, np. zaniku napięcia lub przekroczeniu napięcia znamionowego sieci, przeciążeniu systemu zasilania, lub konieczności wymiany elementów. Minimalny sposób powiadamiania: e-mail, snmp. * System zasilania kompatybilny z dostarczonymi komponentami serwerowymi i macierzowymi min. w zakresie automatycznego zamykania maszyn wirtualnych i wyłączania maszyn sprzętowych w przypadku długotrwałego zaniku napięcia sieciowego. |

### Wymagania minimalne dotyczące routera CE

Tabela 6 Wymagania minimalne dotyczące Routera CE

|  |  |  |
| --- | --- | --- |
| Lp. | Wymaganie | Opis |
|  | Podstawowe wymaganie sprzętowe - 1 | Urządzenie musi być routerem modularnym wyposażonym w min. 7 interfejsów Gigabit Ethernet 10/100/1000 BaseT z czego min. 3 interfejsy muszą pracować jako porty typu WAN oraz min. jeden z interfejsów musi mieć możliwość pracy w trybie DUAL PHYSICAL z min. 1Gb portem światłowodowym definiowanym przez wkładkę SFP. |
|  | Podstawowe wymaganie sprzętowe - 2 | Urządzenie musi być wyposażone w min. 1 GB pamięci FLASH. |
|  | Podstawowe wymaganie sprzętowe - 3 | Urządzenie musi być wyposażone w min. 2 GB pamięci RAM. |
|  | Podstawowe wymaganie sprzętowe - 4 | Urządzenie musi być wyposażone w min. 2 porty USB. Co najmniej jeden z nich musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywanie obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych. Jeden port może pełnić funkcję konsoli szeregowej. |
|  | Architektura – 1 | Urządzenie musi mieć budowę modularną, posiadać możliwość instalacji co najmniej:   * 6 modułów sieciowych z interfejsami Ethernet lub SFP * 1 moduł z układami DSP |
|  | Architektura - 2 | Moduły usługowe muszą mieć możliwość wyłączenia w celu oszczędzania energii elektrycznej. |
|  | Architektura - 3 | Urządzenie musi posiadać zainstalowany, sprzętowy moduł akceleracji szyfrowania DES/3DES/AES |
|  | Architektura - 4 | Urządzenie musi posiadać wszystkie interfejsy „AKTYWNE”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. nie dopuszczalne jest stosowanie karty 4 portowej, gdzie aktywne są 2 porty a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów |
|  | Architektura - 5 | Sloty urządzenia przewidziane pod rozbudowę o dodatkowy moduł muszą mieć możliwość obsadzenia modułami:  z przełącznikiem Ethernetowym gęstości minimum 24 porty na moduł, z portami szeregowymi, z portami FXS, z portami FXO. |
|  | Architektura - 6 | Slot urządzenia przewidziany pod rozbudowę o moduł DSP musi mieć możliwość obsadzenia modułem o gęstości nie mniejszej niż 128 kanałów |
|  | Architektura - 7 | Oczekiwana wydajność routera z włączonymi usługami nie może być mniejsza niż 350 Mbps. |
|  | Architektura - 8 | Oczekiwana wydajność routera dla transmisji ruchu IPsec nie może być mniejsza niż 350 Mbps |
|  | Architektura - 9 | Urządzenie musi obsługiwać jednocześnie min. 3000 tuneli IPsec.. |
|  | Architektura - 10 | Urządzenie musi pozwalać na rozbudowę o funkcjonalność kontrolera WLan za pomocą licencji lub dodatkowego modułu instalowanego w urządzeniu. |
|  | Oprogramowanie – funkcjonalność | Oprogramowanie urządzenia musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności wymiany całego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzanie odpowiednich licencji. |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę protokołów routingu: IPv4, RIPv1, RIPv2, OSPF, ISIS, BGP, ruchu multicastowego: PIM-DM, PIM-SM,PIM-SSM |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę protokołów routingu: IPv6 w tym ICMP dla IPv6,RIPng,BGPv4, OSPFv3, IS-ISv6 |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi wspierać protokół BGP z obsługą 4 bajtowych ASN |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi wspierać funkcjonalności POLICY BASED ROUTING |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać wsparcie dla funkcjonalności związanych obsługą ruchu multicast: IGMPv3, IGMP Snooping, PIMv2 |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF) |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi obsługiwać tzw. routing pomiędzy sieciami VLAN w oparciu o trunking 802.1Q |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, porty TCP/UDP, protokoły IP |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę NAT i PAT dla ruchu IP unicast |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę mechanizmu DiffServ |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę klas ruchu oraz oznaczenie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi zapewniać obsługę mechanizmów kolejkowania ruchu: z obsługą kolejki absolutnego priorytetu, ze statyczną alokacją pasma dla typu ruchu, WFQ |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi obsługiwać mechanizm WRED |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać mechanizm ograniczenia pasma dla określonego typu ruchu |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi obsługiwać protokół NTP |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi obsługiwać DHCP zarówno jako serwer i jako klient |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę tzw. First Hop Redundancy Protocol ( takiego jak HSRP, GLBP, VRRP lub odpowiednika) |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać obsługę protokołów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS oraz TACAS+ lub odpowiednika |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać funkcjonalność firewalla |
|  | Oprogramowanie – funkcjonalność | Urządzenie musi posiadać możliwość zestawiania tuneli VPN z wykorzystaniem protokołu IPsec, IKEv1, IKEv2 |
|  | Zarządzanie i konfiguracja | Urządzenie musi być zarządzalne za pomocą portu konsoli, SSH, telnet, GUI, SNMPv3 |
|  | Zarządzanie i konfiguracja | Urządzenie musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow lub odpowiednika |
|  | Zarządzanie i konfiguracja | Urządzenie musi być zarządzalne za pomocą interfejsu CLI (command line interface) |
|  | Zarządzanie i konfiguracja | Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie offline, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość zapisania co najmniej 10 plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. |
|  | Obudowa | Obudowa urządzenia musi mieć możliwość montażu w szafie RACK. Wysokość obudowy nie większa niż 4U. Wykonawca zobowiązany jest dostarczyć wszelkie elementy montażowe. |
|  | Zasilanie | Urządzenie musi mieć wbudowany zasilacz umożliwiający zasilanie napięciem przemiennym 230V |
|  | Pozostałe | Urządzenie musi być fabrycznie nowe i nieużywane wcześniej, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nie używane przed dniem dostarczenia z wyłączeniem używania niezbędnego do przeprowadzenia testu ich poprawnej pracy |
|  | Pozostałe | Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na rynek Unii Europejskiej a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski. |
|  | Pozostałe | Zamawiający wymaga, aby dostarczone urządzenie posiadało **gwarancję minimum 2 lata**, świadczoną przez Wykonawcę na bazie wsparcia producenta. Wymiana uszkodzonego elementu w trybie min. 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu przekazania przedmiotu zamówienia. |
|  | Pozostałe | Zamawiający wymaga aby przez cały okres gwarancji wszelkie aktualizacje oprogramowania były bezpłatne |

### Wymagania minimalne dotyczące serwera – wariant I

Tabela 7 Wymagania minimalne dotyczące Serwera - wariant I

|  |  |  |
| --- | --- | --- |
| Lp. | Wymagania | Minimalne wymagania dotyczące serwera |
| 1. | Obudowa | Maksymalnie 2U RACK 19” (wraz z wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie). |
| 2. | Płyta główna | Płyta główna dwuprocesowa, musi być kompatybilna z zainstalowanymi podzespołami. Zaprojektowana i wyprodukowana przez producenta serwera. |
| 3. | Parametry procesora | Procesor min. ośmiordzeniowy, wykonany w technologii x86-64, o wydajności pozwalającej na uzyskanie wyniku SPECint\_rate\_base\_2006 nie mniejszej niż 350 pkt (dla serwera, w pełni obsadzonego procesorami). Zamawiający może zażądać dostarczenia wyników w/w testów. |
| 4. | Ilość procesorów | Min. 1 |
| 5. | Pamięć RAM | Min. 32GB pamięci RAM DDR4 z korekcją błędów ECC. Kości pamięci o pojemności minimalnej 16GB. Możliwość Instalacji w serwerze min. 1TB pamięci RAM. |
| 6. | Podsystem dyskowy | Min. 2x min. 300GB SAS 10k RPM lub szybsze np. SSD. Zainstalowany kontroler macierzowy SAS zapewniający obsługę RAID na poziomie 0/1/10,5,50,6,60. Moduł pomięci cache minimum 1GB wyposażony w podtrzymywanie zawartości pomięci typu flash. |
| 7. | Karty sieciowe | Minimum dwie karty Ethernet zapewniające min po dwa interfejsy (każda karta) 10Gb SFP+ wraz z min. 4 modułami optycznymi typu SR. Dodatkowa karta 1Gb Ethernet z min. 2 interfaceami.  Zamawiający wymaga aby serwery były podłączone bezpośrednio za pomocą kabli przyłączeniowych do macierzy – Wykonawca musi dostarczyć odpowiednie kable i interfacey sieciowe zarówno do serwerów jak i macierzy, jeśli zaproponowane rozwiązanie wymaga podłączenia za pośrednictwem dodatkowego przełącznika sieciowego, Wykonawca musi to uwzględnić w ofercie. |
| 8. | Sloty rozszerzeń | Minimum dwa sloty PCI-Express 3.0. możliwość rozbudowy do minimum 6 slotów PCI-Express 3.0, w tym minimum dwa sloty PCI-Express Generacji 3.0x16 (prędkość slotu – buswidth) pełnej wysokości. |
| 9. | Porty USB | Minimum 4 porty USB ( w tym co najmniej dwa w wersji 3.0) |
| 10. | Zasilacze | Minimum 2 szt., redundantne, typu hot-plug |
| 11. | Zarządzanie i obsługa techniczna | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Wymagane dostarczenie funkcjonalności przejęcie zdalnej konsoli graficznej i podłączenia wirtualnych napędów DVD/ISO, współdzielenie konsoli pomiędzy kilku użytkowników. Dostęp z poziomu przeglądarki WWW jak i z linii komend CLI. Karta z dedykowanym portem RJ-45. Rozwiązywanie sprzętowe niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. Zdalna identyfikacja fizycznego serwera i odbudowy za pomocą sygnalizatora optycznego. |
| 12. | Wsparcie serwisowe | Min. 2 lata w trybie min. 9 godz./5dni. Gwarantowany czas reakcji zgodny z SLA dla projektu. Naprawa w lokalizacji Zamawiającego. Z możliwością przedłużenia. |

### Wymagania minimalne dotyczące serwera – wariant II

Tabela 8 Wymaganie minimalne dotyczące serwera - wariant II

|  |  |  |
| --- | --- | --- |
| Lp. | Wymagania | Minimalne wymagania dotyczące serwera |
| 1. | Obudowa | Maksymalnie 2U RACK 19” (wraz z wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie). |
| 2. | Płyta główna | Płyta główna dwuprocesowa, musi być kompatybilna z zainstalowanymi podzespołami. Zaprojektowana i wyprodukowana przez producenta serwera. |
| 3. | Parametry procesora | Procesor min. ośmiordzeniowy, wykonany w technologii x86-64, o wydajności pozwalającej na uzyskanie wyniku SPECint\_rate\_base\_2006 nie mniejszej niż 400 pkt (dla serwera, w pełni obsadzonego procesorami). Zamawiający może zażądać dostarczenia wyników w/w testów. |
| 4. | Ilość procesorów | Min. 2 |
| 5. | Pamięć RAM | Min. 64GB pamięci RAM DDR4 z korekcją błędów ECC. Kości pamięci o pojemności minimalnej 32GB. Możliwość Instalacji w serwerze min. 1TB pamięci RAM. |
| 6. | Podsystem dyskowy | Min. 2x min. 300GB SAS 10k RPM lub szybsze np SSD. Zainstalowany kontroler macierzowy SAS zapewniający obsługę RAID na poziomie 0/1/10,5,50,6,60. Moduł pomięci cache minimum 1GB wyposażony w podtrzymywanie zawartości pomięci typu flash. |
| 7. | Karty sieciowe | Minimum dwie karty Ethernet zapewniające min po dwa interfejsy (każda karta) 10Gb SFP+ wraz z min. 4 modułami optycznymi typu SR. Dodatkowa karta 1Gb Ethernet z min. 2 interfaceami.  Zamawiający wymaga aby serwery były podłączone bezpośrednio za pomocą kabli przyłączeniowych do macierzy – Wykonawca musi dostarczyć odpowiednie kable i interfacey sieciowe zarówno do serwerów jak i macierzy, jeśli zaproponowane rozwiązanie wymaga podłączenia za pośrednictwem dodatkowego przełącznika sieciowego, Wykonawca musi to uwzględnić w ofercie. |
| 8. | Sloty rozszerzeń | Minimum dwa sloty PCI-Express 3.0. możliwość rozbudowy do minimum 6 slotów PCI-Express 3.0, w tym minimum dwa sloty PCI-Express Generacji 3.0x16 (prędkość slotu – buswidth) pełnej wysokości. |
| 9. | Porty USB | Minimum 4 porty USB ( w tym co najmniej dwa w wersji 3.0) |
| 10. | Zasilacze | Minimum 2 szt., redundantne, typu hot-plug |
| 11. | Zarządzanie i obsługa techniczna | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Wymagane dostarczenie funkcjonalności przejęcie zdalnej konsoli graficznej i podłączenia wirtualnych napędów DVD/ISO, współdzielenie konsoli pomiędzy kilku użytkowników. Dostęp z poziomu przeglądarki WWW jak i z linii komend CLI. Karta z dedykowanym portem RJ-45. Rozwiązywanie sprzętowe niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCl. Zdalna identyfikacja fizycznego serwera i odbudowy za pomocą sygnalizatora optycznego. |
| 12. | Gwarancja | Min. 2 lata w trybie min. 9 godz./5dni. Gwarantowany czas reakcji zgodny z SLA dla projektu. Naprawa w lokalizacji Zamawiającego. Z możliwością przedłużenia. |

### Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych

Tabela 9 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych

|  |  |  |
| --- | --- | --- |
| Lp. | Wymagania | Minimalne wymagania dotyczące macierzy |
| 1. | Obudowa | Obudowa do montażu w szafir rack 19” z pomocą dostarczonych dedykowanych elementów. |
| 2. | Kontrolery dyskowe | Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active/active. Możliwość rozbudowy do 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączenie kilku macierzy przez wirtualizator zasobów dyskowych). |
| 3. | Wymagana przestrzeń | Fizyczna przestrzeń dyskowa zbudowana za pomocą minimum 9 dysków o pojemności nie mniejszej niż 1,2 TB SAS 10 RPM lub szybszych, np. SSD. Zamawiający wymaga aby awaria 1 dysku nie powodowała utraty danych, zmniejszenia pojemności netto macierzy oraz zmniejszenia parametrów optymalnych dla pracy z bazami danych (wydajność). Wymagana przestrzeń netto macierzy min. 3,5 TB. |
| 4. | Możliwość rozbudowy macierzy | Rozbudowa oferowanej macierzy do co najmniej 500 napędów dyskowych, bez wymiany kontrolerów macierzowych (tylko poprzez dodanie półek i napędów dysków). W ramach macierzy musi być możliwa instalacja półek dyskowych obsadzonych różnymi rodzajami dysków, np. PCIe SSD w jednej półce i SATA w drugiej. |
| 5. | Pamięć cache | Min. 16 GB pamięci cache na każdy kontroler, pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości w pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min 48 godzin. Możliwość rozbudowy do 128 GB. Rozbudowa nie może odbywać się poprzez pamięć FLASH/SSD. |
| 6. | Zabezpieczanie dyskami SPARE | Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |
| 7. | Dostępne interfejsy | Razem kontrolery muszą udostępnić minimum 4 interfejsy 1 Gb/s ETH i min. 4 interfejsy 10Gb/s do podłączenia serwerów. Możliwość rozbudowy o dodatkowe 8 interfejsów FC 8Gb/s lub 8 interfejsów FC 16Gb/s lub 8 interfejsów 10Gb/s ETH. |
| 8. | Obsługiwane typy zabezpieczenia RAID | Kontrolery wyposażone w funkcjonalność konfiguracji poziomów RAID, min: RAID 0, RAID 1, RAID 10, RAID 5, RAID 6. Zabezpieczenia RAID realizowane za pomocą sprzętowego dedykowanego układu, z możliwością ich kombinacji w/w typów w ramach oferowanej macierzy. |
| 9. | prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (ang. Thin Provisioning) | Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowa (ang. Thin Provisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space reclamation). |
| 10. | Migracja danych wolumenu logicznego pomiędzy różnymi technologiami dyskowymi (ang. Tiering) | Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych (ang. Tiering) na poziomie całych woluminów logicznych lub jego fragmentów, w szczególności macierz musi zapewniać zmianę poziomu RAID/migrację danych bez konieczności rekonfiguracji po stronie serwerów korzystających z woluminów logicznych. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania. |
| 11. | Podłączenie zewnętrznych systemów operacyjnych | Możliwość jednoczesnego podłączania co najmniej 30 niezależnych systemów HP-UX, Vmware, Linux i MS Windows |
| 12. | Serwisowalność | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania. Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii. |
| 13. | Zrządzanie | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową. |
| 14. | Kopie wewnątrz macierzy | Tworzenie na żądanie tzw. migawkowej kopii danych (ang. Snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów systemów komputerowych. Wymagane jest dostarczenie w/w funkcjonalności.  Tworzenie na żądanie pełnej fizycznej kopii danych (klon) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wymagana jest możliwość kopiowania pomiędzy obszarami danych zabezpieczonych różnymi poziomami RAID.  Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania. |
| 15. | Replikacja danych | Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie synchronicznym i asynchronicznym. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania. |
| 16. | Klaster macierzowy | Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage metro cluster) pozwalające na uruchomienie środowiska wysokiej dostępności (tryb activ-activ) zbudowanego z dwóch macierzy dyskowych.  Dostarczenie wszystkich komponentów sprzętowych do uruchomienia w/w funkcjonalności dla środowisk wirtualizacyjnych.  Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania. |
| 17. | Wsparcie serwisowe | Min. 2 lata w trybie 9godzin/5dni. Gwarantowany czas reakcji zgodny z SLA dla projektu. Naprawa w lokalizacji Zamawiającego. Z możliwością przedłużenia. |

### Stanowiska robocze

#### Stanowisko robocze – komputer stacjonarny i monitor

Tabela 10 Wymagania minimalne dotyczące komputera stacjonarnego z monitorem

|  |  |
| --- | --- |
| Komputer | * Procesor: min 2 rdzeniowy, osiągający wynik min. 4500 pkt w teście PassMark - CPU Mark [11.2017] * RAM min. 8 GB * HDD min. 500GB * Karta graficzna - min. zintegrowana * Bez napędu optycznego * Komunikacja: Lan 10/100/1000, WIFI ac/a/b/g/n * Stan: Nowy nieużywany, Wersja fabryczna |
| Monitor | * minimum 21,5”, LCD * podświetlenie LED * proporcje ekranu 16:9 * Rozdzielczość normatywna matrycy: min 1920 x1080 |
| Wyposażenie dodatkowe | * klawiatura + mysz USB * preinstalowany system operacyjny dedykowany do zastosowań desktop w wersji umożliwiającej podłączenie do domeny Active Directory oraz uruchomienie SD bez użycia wirtualizacji. * pakiet oprogramowania biurowego (edytor, arkusz, poczta) obsługujący w 100% zgodny z MS Office standardy dokumentów docx, xlsx, pptx * program antywirusowy zarządzany z centralnej konsoli |
| Wsparcie serwisowe | min. 2 lata w trybie 9godzin/5dni. Gwarantowany czas reakcji zgodne z SLA dla projektu. Naprawa w lokalizacji Zamawiającego. Z opcją przedłużenia. |

#### Stanowisko robocze – laptop

Tabela 11 Wymagania minimalne dotyczące komputera przenośnego typu laptop

|  |  |
| --- | --- |
| Komputer | * przenośny * procesor: min 2 rdzeniowy, osiągający wynik min. 4500 pkt w teście PassMark - CPU Mark Laptop & Portable CPU Performance [11.2017] * pamięć RAM: min. 8 GB * HDD min. 1 TB * Min. 2 x USB 3.0 * czas pracy na baterii: min 4 h * Komunikacja: Lan 10/100/1000, WIFI ac/a/b/g/n |
| Ekran | * min 15” LCD max. 17” * podświetlenie LED * proporcje ekranu 16:9 |
| Wyposażenie dodatkowe | * preinstalowany system operacyjny dedykowany do zastosowań desktop w wersji umożliwiającej podłączenie do domeny Active Directory oraz uruchomienie SD bez użycia wirtualizacji. * pakiet oprogramowania biurowego (edytor, arkusz, poczta) obsługujący w 100% zgodny z MS Office standardy dokumentów docx, xlsx, pptx * program antywirusowy zarządzany z centralnej konsoli * Mysz bezprzewodowa, torba na laptopa. |
| Wsparcie serwisowe | min. 2 lata w trybie 9godzin/5dni. Gwarantowany czas reakcji zgodne z SLA dla projektu. Naprawa w lokalizacji Zamawiającego. Z opcją przedłużenia. |

#### Wymagania minimalne dotyczące skanera małego

Tabela 12 Wymagania minimalne dotyczące parametrów skanera małego

|  |  |
| --- | --- |
| Parametr | Minimalne wartości parametru |
| Typ skanera | Dokumentowy (Duplex), A4 |
| Źródło światła | LED |
| Podawanie papieru | Automatyczne z duplexem, min. 80 arkuszy |
| Gramatura papieru | min. 30 - 400 g/m2 |
| Optyczna rozdzielczość | min. 600 dpi |
| Rozdzielczość wyjściowa | min. od 50 do 600 dpi |
| Rozmiar dokumentów | Maks. 216 mm x 356 mm |
|  | Min nie większe niż 81x81 mm |
| Skanowanie długich dokumentów | Do min. 3 m (kolor, min. 300 dpi, duplex) |
| Prędkość skanowania | min. 30 PPM / 60 IPM (dla: kolor, B&W, A4, 300 dpi) |
|  | min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 200 dpi) |
| Głębia koloru | min. 24 bit wyjściowe |
| Skala szarości | min. 8 bit wyjściowe |
| Interfejs | min. USB 2.0 |
| Zasilanie | 240 V AC, 50Hz |
| Sugerowana obciążalność dzienna | min. 5000 stron |
| Obsługiwane systemy operacyjne | Windows 7/8/8.1/10 |
| Wykrywanie błędów | Czujnik ultradźwiękowy |
| Wymiary urządzenia | Max. 320 mm x 220 mm x 250 mm (szerokość x głębokość x wysokość) |
| Masa | max. 4,5 kg |
| Gwarancja | Min. 2 lata |

#### Wymagania dotyczące skanera dużego

Tabela 13 Wymagania minimalne dotyczące parametrów skanera dużego

|  |  |
| --- | --- |
| Typ skanera | Dokumentowy (Duplex) A4 |
| Źródło światła | LED |
| Podawanie papieru | ADF min. 80 arkuszy |
| Gramatura papieru | min. 30 - 400 g/m2 |
| Optyczna rozdzielczość | min. 600 dpi |
| Rozdzielczość wyjściowa | min. od 50 do 600 dpi |
| Rozmiar dokumentów | Maks. 216 mm x 356 mm |
|  | Min. nie większe niż 81x81 mm |
| Skanowanie długich dokumentów | Do min. 3 m (kolor, min. 300 dpi, duplex) |
| Prędkość skanowania | min. 40 PPM / 80 IPM (dla: kolor, B&W, A4, 300 dpi) |
|  | min. 60 PPM / 120 IPM (dla: kolor, B&W, A4, 200 dpi) |
| Głębia koloru | min. 24 bit wyjściowe |
| Skala szarości | min. 8 bit wyjściowe |
| Interfejs | min. USB 2.0 |
| Zasilanie | 240 V AC, 50Hz |
| Sugerowana obciążalność dzienna | min. 6000 stron |
| Obsługiwane systemy operacyjne | Windows 7/8/8.1/10 |
| Wykrywanie błędów | Czujnik ultradźwiękowy |
| Wymiary urządzenia | Max. 320 mm x 220 mm x 250 mm (szerokość x głębokość x wysokość) |
| Masa | max. 4,5 kg |
| Gwarancja | min. 2 lata |

#### Wymagania dotyczące drukarki etykiet

Tabela 14 Wymagania minimalne dotyczące parametrów drukarki etykiet

|  |  |
| --- | --- |
| Parametr | Minimalne wartości parametru |
| Dostępne interfejsy: | min. USB, Ethernet (LAN) |
| Rozdzielczość druku [dpi]: | min. 200 |
| Rodzaj druku: | termiczny |
| Maks. prędkość druku [mm/s]: | min. 120 |
| Wymiary [mm] WxHxL: | max: 255 x 255 x 255 |
| Min. szerokość etykiet [mm]: | max. 25 |
| Szerokość druku [mm]: | min. 100 |
| Maks. długość druku [mm]: | min. 200 |
| Zasilanie: | AC: 230V / 50 Hz |
| Maksymalna szerokość etykiety [mm]: | min. 110 |
| Maksymalna wysokość etykiety [mm]: | min. 210 |
| Gwarancja | min. 2 lata |

#### Wymagania dotyczące skanera kodów kreskowych

Tabela 15 Wymagania minimalne dotyczące parametrów skanerów kodów kreskowych

|  |  |
| --- | --- |
| Parametr | Minimalne wartości parametru |
| Rodzaje interfejsu: | min. USB, PS/2 |
| Typ skanera: | 1D lub 1/2D |
| Odczytywane kody kreskowe: | min: UPC/EAN: UPC-A, UPC-E, UPC-E1, EAN-8/JAN 8, EAN-13/JAN 13, Bookland EAN, Bookland ISBN Format, UCC Coupon Extended Code, ISSN EAN Code 128, w tym GS1-128, ISBT 128, ISBT Concatenation, Code 39, Code 39 Full ASCII Conversion Code 93 Code 11 Matrix 2 of 5 Interleaved 2 of 5 (ITF) Discrete 2 of 5 (DTF) Codabar GS1 DataBar, w tym GS1 DataBar-14, GS1 DataBar Limited, GS1 DataBar Expanded GS1 DataBar, GS1 DataBar-14,GS1 DataBar Limited, GS1 DataBar Expanded |
| Zasięg odczytu: | min. 5m |
| Szybkość skanowania: | min. 500 skanów/sek. |
| Sygnalizacja odczytu: | dźwiękowa i świetlna |
| Odporność na upadki: | min. do 1,5m |
| Norma szczelności: | Zabezpieczony przeciwko działaniu kurzu |
| Zasięg pracy od bazy komunikacyjno-ładującej: | min. 50m |
| Gwarancja | min. 2 lata |

### Wymagania minimalne dotyczące przełączników sieciowych

Tabela 16 Wymagania minimalne dotyczące przełączników sieciowych

|  |  |
| --- | --- |
| Lp. | Opis wymogu |
| 1. | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie RACK. Wymagane jest dostarczenie z przełącznikiem zestawu montażowego wraz z przewodami i patchcordami. |
| 2. | Wymagane parametry fizyczne:   1. wysokość maksymalna 1U 2. wewnętrzny redundantny zasilacz 230V AC. 3. Zakres temperatur pracy ciągłej minimum 0 – 45 stopni Celsjusza 4. Co najmniej jeden port USB umożliwiający podłączenia zewnętrznej pamięci FLASH |
| 3. | Przełącznik musi posiadać :   1. Minimum 48 portów 10/100/1000Base-T 2. Minimum 4 porty 10G SFP 3. Urządzenie musi umożliwiać wykorzystanie min. 52 portów. Jeżeli do obsługi wymaganych portów potrzebna jest licencja to należy ją dostarczyć w ramach niniejszego postępowania. Licencja na użytkowanie musi być bezterminowa. |
| 4. | Porty 10G SFP muszą mieć możliwość obsługi standardów 10GBase –LX, 10GBase-SX, kable DAC o długości min. 1m. Do każdego przełącznika należy dostarczyć 2 wkładki SFP 10G-SX oraz 2 wkładki 1G-SX. Wkładki SFP muszą pochodzić od producenta oferowanych przełączników w celu zapewnienia najlepszej kompatybilności oraz muszą być objęte takim samym wsparciem technicznym i serwisowym jak oferowane przełączniki. Oferowane wkładki muszą być kompatybilne z wkładkami serwerowymi i macierzowymi. |
| 5. | Przełącznik musi posiadać funkcjonalność łączenia w stosy z zachowaniem następującej funkcjonalności   1. Do min. 6 jednostek w stosie 2. Zarządzanie stosem przez jeden adres IP 3. Magistrala stakująca o przepustowości min. 80Gbps 4. Możliwość tworzenia połączeń link agregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (cross – stack link agregation) 5. Stos przełączników powinien być widziany w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree 6. Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych modułów, przewodów lub licencji stakujących to w ramach niniejszego postepowania Zamawiający wymaga ich dostarczenia. Zamawiający dopuszcza aby możliwość łączenia w stosy była realizowana przy użyciu portów typu UPLINK [przy zachowaniu min. przepustowości oraz zajęciu nie więcej jak 4 portów]. Zamawiający wymaga dostarczenia kabli stakujących o długości 1 m do każdego urządzenia. |
| 6. | Matryca przełączająca o wydajności min.330Gbps, wydajność przełączania min.78 Mpps |
| 7. | Wbudowana pamięć RAM min 512 MB. |
| 8. | Wbudowana pamięć FLASH min. 200 MB |
| 9. | Obsługa min. 16000 adresów MAC |
| 10. | Obsługa min. 400 sieci Vlan jednocześnie oraz obsługa 802.1Q tuneling (QinQ). |
| 11. | Obsługa ramek JUMBO o wielkości min. 9216 B. |
| 12. | Możliwość skonfigurowania min. 1024 interfejsów Vlan interface SVI działających równocześnie. |
| 13. | Obsługa protokołu GVRP |
| 14. | Wsparcie dla protokołu IEEE 802.1 w Rapid Spanning Tree oraz IEEE 802.1s Multi Instance Spanning Tree. Wymagane wsparcie dla min 64 instancji protokołu MSTP. |
| 15. | Obsługa min. 8000 tras dla routingu IPv4 |
| 16. | Obsługa min. 2000 tras dla routingu IPv6 |
| 17. | Obsługa min. 3000 tras dla routingu statycznego IPv4 |
| 18. | Obsługa min. 1000 tras dla routingu statycznego IPv6 |
| 19. | Obsługa min. 64 wirtualnych tablic routingu-forwardingu (VRF) |
| 20. | Przełącznik musi posiadać funkcjonalność DHCP serwer |
| 21. | Obsługa protokołów LLDP i LLDP - MED |
| 22. | Obsługa ruchu multicast – IGMP v1, v2, v3 |
| 23. | Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:   1. Min. 4 poziomy dostępu administracyjnego poprzez konsolę 2. Automatyzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału Vlan oraz dynamicznego przypisania listy ACL 3. Możliwość uwierzytelniania urządzenia w oparciu o adres MAC oraz poprzez wbudowany portal WWW 4. Zarządzanie urządzeniem poprzez HTTPS, SNMP, SSH za pomocą protokołów IPv4 i IPv6 5. Możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP 6. Obsługa mechanizmów Port Security, Dynamic ARP inspection, IP Source Guard, voice Vlan oraz private Vlan ( lub równoważny). 7. Możliwość synchronizacji czasu z serwerem NTP |
| 24. | Obsługa funkcjonalności UDLD lub równoważnej |
| 25. | Implementacja min. 8 kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach – klasyfikacja ruchu dla klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP |
| 26. | Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia pakietów UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi mieć możliwość konfiguracji liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga oddzielnej licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania. Licencja musi być ważna min. przez okres trwałości projektu. |
| 27. | Wymagane opcje zarządzania:   1. Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony Vlan 2. Zamawiający wymaga aby istniała możliwość zapisu pliku konfiguracyjnego i następnie jego edycji w trybie off-line. Konieczna jest możliwość edycji konfiguracji w pliku tekstowym a następnie zapisania zmian przy użyciu dowolnego urządzenia PC. 3. Dedykowany port konsoli oraz dedykowany port zarządzający out-of-band min. 10/100Base-T |
| 28. | Z urządzeniem musi być dostarczona pełna dokumentacja w języku polskim lub angielskim. |
| 29. | Urządzenie musi być fabrycznie nowe i nieużywane wcześniej, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nie używane przed dniem dostarczenia z wyłączeniem używania niezbędnego do przeprowadzenia testu ich poprawnej pracy |
| 30. | Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na rynek Unii Europejskiej a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski. |
| 31. | Zamawiający wymaga, aby dostarczone urządzenie posiadało gwarancję minimum 2 lata, świadczoną przez Wykonawcę na bazie wsparcia producenta. Wymiana uszkodzonego elementu w trybie zgodnym z SLA dla Projektu. Okres gwarancji liczony będzie od daty sporządzenia protokołu przekazania przedmiotu zamówienia. |
| 32. | Zamawiający wymaga aby przez cały okres gwarancji wszelkie aktualizacje oprogramowania były bezpłatne |

### Wymagania minimalne dotyczące oprogramowania do wirtualizacji serwerów lokalnych

* 1. Licencje muszą umożliwiać uruchamianie wirtualizacji na serwerach fizycznych bez ograniczeń na ilość procesorów oraz rdzeni lub zapewniać obsługę maksymalnej możliwej do zainstalowania ilości procesorów z minimum 12 rdzeniami każdy oraz jednej konsoli do zarządzania całym środowiskiem. (uwaga: po jednej konsoli dla każdej z lokalizacji terenowych).
  2. Wszystkie licencje powinny być dostarczone wraz z 5 -letnim wsparciem technicznym na poziomie podstawowym. Licencja ma zapewniać możliwość wieczystej własności.
  3. Wymagania techniczne i funkcjonalne dot. oprogramowania:

- c 1) Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

- c 2) Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej:

* Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w min. 320 logicznych wątków oraz do min. 4TB pamięci fizycznej RAM,
* Oprogramowanie do wirtualizacji musi zapewniać możliwość skonfigurowania maszyn wirtualnych min. 1-64 procesorowych,
* Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do min. 62 TB,
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do min. 1 TB pamięci operacyjnej RAM,
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć min. 1-10 wirtualnych kart sieciowych,
* Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć co najmniej: 2 porty szeregowe i 2 porty równoległe i 20 urządzeń USB,
* Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług,
* Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej,
* Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami rożnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą. Licencjonowanie nie może odbywać się w trybie OEM,
* Rozwiązanie musi wspierać następujące systemy operacyjne: Windows Server 2008, Windows Server 2012, Windows Server 2016, SLES od wersji 8, RHEL od wersji 3, Solaris od wersji 8, Debian, CentOS, FreeBSD, Mandriva, Ubuntu od wersji 12.04, SCO OpenServer, SCO Unixware, Mac OS X,
* Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno, jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance,
* Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystana zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane min. sprzed roku,
* Oprogramowanie do wirtualizacji powinno zapewniać możliwość wykonywania kopii migawkowych instalacji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerwania ich pracy,
* Oprogramowanie do wirtualizacji musi zapewniać możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi,
* Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory,
* Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn,
* Rozwiązanie musi wspierać mechanizmy do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewniać stosowanie deduplikacji dla kopii zapasowych,
* System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów,
* Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
  1. Wymagania ogólne dotyczące oprogramowania do zarządzania maszynami wirtualnymi:
     + Oprogramowanie musi współpracować z dostarczoną infrastrukturą
     + Oprogramowanie musi współpracować z hostami zarządzanymi wspólnie oraz pojedynczymi hostami.
     + Oprogramowanie musi współpracować z hostami pracującymi w klastrze hostów oraz pojedynczymi hostami.
     + Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych .
  2. Całkowite koszty posiadania:
* Oprogramowanie musi być licencjonowanie w modelu „per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone
* Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć „samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi posiadać mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla podstawowych funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi zapewniać backup jednoprzebiegowy – nawet w przypadku wymagania granularnego odtworzenia
* Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku Vmware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji,
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
  1. Wymagania RPO
* Oprogramowanie musi wykorzystywać mechanizmy Chenge Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi wspierać kopiowanie na taśmy
* Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape serwer
* Oprogramowanie musi kopiowania backupów lokalizacji zdalnej
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
* Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn.
* Oprogramowanie musi umożliwiać przechowywania punktów przywracania replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
* Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego
* Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie ( paralel procesing)
  1. Wymagania RTO
* Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności – oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć,
* Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
* Linux: ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
* BSD: UFS, UFS2
* Solaris: ZFS, UFS
* Mac: HFS, HFS+
* Windows: NTFS, FAT, FAT32, ReFS
* Novell OES: NSS
  + - Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
    - Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej
    - Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
    - Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze „Permanently Deleted Objects”).
    - Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2010 i nowsze
    - Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia
    - Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
    - Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
    - Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym „reverse CBT” oraz odtwarzanie z wykorzystaniem sieci SAN

## Modernizacja sieci LAN

### Informacje ogólne

W ramach projektu przewiduje się modernizację sieci LAN (aktywnej i pasywnej) w poszczególnych JST. Modernizacja sieci będzie miała za zadanie zbudowanie punktu styku z siecią szkieletową (zapewnia operator), który będą stanowić przełączniki szkieletowo-dystrybucyjne oraz punktów dostępowych do sieci LAN.

Przyłącza pasywne do sieci szkieletowej powinny w każdej lokalizacji JST zostać wyprowadzone na przełącznicę światłowodową umieszczoną w MDF. System okablowania strukturalnego dla sieci LAN powinien tworzyć niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działania obecnych i przyszłych aplikacji.

W lokalizacjach Zamawiającego zapewnione są warunki niezbędne do zainstalowania i pracy urządzeń a w szczególności zapewniono wymagane przez producenta warunki eksploatacji urządzeń - zamawiający musi udostępnić infrastrukturę kablową, która po modernizacji PEL spełni wymagania normy ISO/IEC 11801, ANSI/TIA/EIA-568, PN-EN 50173, Zamawiający zapewnia także zasilanie niezbędne do funkcjonowania urządzeń oraz miejsce w szafach Rack. Zakresy prac niezbędne do wykonania w ramach poszczególnych jednostek terenowych określają szkice organizacji sieci LAN stanowiące Załącznik nr 9 do SIWZ. W przypadku wątpliwości dot. załączonych szkiców każdorazowo Wykonawca ustali szczegóły z Administratorem Sieci LAN w jednostce terenowej partnera.

W przypadku lokalizacji 1 [Starostwo Powiatowe w Giżycku] wymagane jest połączenie w logiczną całość sieci znajdujących się w obu budynkach partnera. Połączenie to nie może być wykonane za pomocą sieci bezprzewodowych i nie może wymagać użycia elementów aktywnych w torze kablowym [np., wzmacniaczy, repeaterów, itp.].

Tabela 17 Wymagania minimalne dotyczące prac w ramach modernizacji sieci LAN

|  |  |
| --- | --- |
| Kod | Wymaganie |
| WSZL21 | Instalacja gniazd natynkowych PEL.  Zamawiający wymaga wykonania instalacji nowych/modernizacji/naprawy gniazd PEL (punkty elektryczno logiczne) w lokalizacjach 1,2,6,8,10. Liczba PEL określona jest w tabeli 1.1 |
| WSZL22 | Zamawiający wymaga wykonania całej infrastruktury w kategorii min. 5E. |
| WSZL23 | Zamawiający wymaga minimalnej struktury PEL : 1 gniazdo RJ45 + 1 gniazdo 230V. Wszystkie gniazda RJ45 zakończone we wskazanych przez zamawiającego serwerowniach / szafach dystrybucyjnych RACK na patchpanelach kat min. 5E. |

### Przewidywany zakres prac

W ramach instalacji okablowania strukturalnego przewidziano następujące prace:

* budowę/modernizację tras kablowych,
* układanie kabli w nowych i istniejących trasach,
* instalacja punktów PEL (punkt elektryczno-logiczny),
* montaż paneli krosowych RJ45 w szafach w punktach dystrybucyjnych,
* montaż przyłączy światłowodowych,
* terminowanie przyłączy światłowodowych,
* dostarczenie i montaż do szafy telekomunikacyjnej, przełącznic światłowodowych, patchpaneli krosowych RJ45 min. kat. 5E, Ilość paneli należy dostosować do liczby instalowanych gniazd z zapewnieniem 50% nadmiarowości
* terminowanie kabli w osprzęcie przyłączeniowym,
* pomiary tras kablowych, wykonanie dokumentacji powykonawczej

### Zakres usług utrzymania sieci LAN w JST

Za utrzymanie warstw systemu tj. :

* sprzętowej (serwery, macierzy dyskowych, elementy sieciowe aktywne i pasywne ),
* system backup,
* oprogramowana do wirtualizacji,
* wszystkie serwery wirtualne wymagane do prawidłowego funkcjonowania sieci,

**odpowiada Wykonawca**

* oprogramowania systemowego klienta (systemy operacyjne),
* Active Directory,

**odpowiada Zamawiający**

## Instalacja, konfiguracja i uruchomienie publicznych punktów dostępowych WiFi

### Informacje ogólne

Wszystkie punkty dostępowe zostaną rozmieszczone na terenie oraz wokół poszczególnych budynków urzędów administracji samorządowej biorącej udział w projekcie oraz wybranych lokalizacjach na terenie miejscowości. Punkty te pozwolą na dostęp do zasobów teleinformatycznych oraz usług elektronicznych uruchomionych w ramach projektu użytkownikom korzystającym z urządzeń mobilnych, zarówno pracownikom administracji samorządowej, jak również klientom administracji.

### Miejsce instalacji punktów

Wykonawca w porozumieniu z Zamawiającym ustali dokładne lokalizacje miejsc instalacji i sposobu ich wykonania po podpisaniu umowy. Przewidywane miejsca instalacji zamieszczono w poniższej tabeli:

Tabela 18 Przewidywane miejsca instalacji punktów WiFi

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp | JST | Jednostka | Adres lokalizacji | Działka |
| 1 | Gmina Miejska Giżycko | MOSiR Stadion | 11-500 Giżycko, ul. Moniuszki 5 | 356 obręb 1 |
| 2 | Gmina Miejska Giżycko | MOSiR Stadion | 11-500 Giżycko, ul. Moniuszki 5 | 356 obręb 1 |
| 3 | Gmina Miejska Giżycko | Urząd Miejski | 11-500 Giżycko, Al. 1 Maja 14 | 470 obręb 2 |
| 4 | Gmina Miejska Giżycko | Szkoła Podstawowa Nr 7 | 11-500 Giżycko, Wodociągowa 8 | 1310 obręb 2 |
| 5 | Gmina Miejska Giżycko | Miejski Ośrodek Pomocy Społecznej | 11-500 Giżycko, Wodociągowa 15 | 1062/9 obręb 2 |
| 6 | Gmina Miejska Giżycko | MOSiR Pływalnia | 11-500 Giżycko, ul. Sikorskiego 3c | 589/1 obręb 2 |
| 7 | Gmina Miejska Giżycko | Szkoła Podstawowa Nr 4 | 11-500 Giżycko, ul. 3 Maja 21 | 585/4 obręb 2 |
| 8 | Gmina Miejska Giżycko | Zespół Szkół Nr 1 | 11-500 Giżycko, ul. Wiejska 50 | 716/1 obręb 3 |
| 9 | Gmina Miejska Giżycko | Gimnazjum Nr 2 | 11-500 Giżycko, ul. Warszawska 39 | 257/4 obręb 2 |
| 10 | Gmina Miejska Giżycko | Gimnazjum Nr 1 | 11-500 Giżycko, ul. Gimnazjalna 1 | 451/3 obręb 2 |
| 11 | Starostwo Powiatowe w Giżycku | Schronisko Młodzieżowe :Zofiówka: | 11-520 Ryn, ul. Mazurska 19 | 1/14, 1/16, 1/76 obręb 0001 Miasto Ryn |
| 12 | Gmina Ryn | Urząd Miasta i Gminy | 11-520 Ryn, ul. Świerczewskiego 2 | 126/18 obręb 01 Miasto Ryn |
| 13 | Gmina Ryn | Przedszkole miejskie | 11-520 Ryn, ul. Świerczewskiego 2 | 141/21 obręb 01 Miasto Ryn |
| 14 | Gmina Ryn | Stanica Wodna EKOMARINA | 11-520 Ryn, ul. Hanki Sawickiej 7A | 47/4 obręb 01 Miasto Ryn |
| 15 | Gmina Ryn | Plaża miejska | 11-520 Ryn, ul. Konrada Wallenroda | 76/11 obręb 01 Miasto Ryn |
| 16 | Gmina Ryn | Targowisko Miejskie | 11-520 Ryn, Plac Wolności | 72/46 obręb 01 Miasto Ryn |
| 17 | Gmina Ryn | Boisko Orlik | 11-520 Ryn, ul. Hanki Sawickiej | 366 obręb 01 Miasto Ryn |
| 18 | Gmina Ryn | Remiza OSP Sterławki Wlk. | 11-520 Ryn, Sterławki Wielkie 54 | 140 obręb 15 Gmina Ryn |
| 19 | Gmina Ryn | Remiza OSP Ryn | 11-520 Ryn, ul. Zielona 3 | 87 obręb 01 Miasto Ryn |
| 20 | Gmina Miłki | Urząd Gminy | 11-513 Miłki, ul. Mazurska 2 | 16 obręb Miłki |
| 21 | Gmina Ruciane-Nida | Urząd Miasta i Gminy | 12-220 Ruciane-Nida, Aleja Wczasów 4 | 133/3 obręb Ruciane-Nida |
| 22 | Gmina Ruciane-Nida | Informacja Turystyczna | 12-220 Ruciane-Nida, ul. Dworcowa 14 | 106/3 obręb Ruciane-Nida |
| 23 | Gmina Ruciane-Nida | Szkoła Podstawowa Nr 1 | 12-220 Ruciane-Nida, ul. Gałczyńskiego 2 | 269 obręb Ruciane-Nida |
| 24 | Gmina Pozezdrze | Urząd Gminy | 11-610 Pozezdrze, al.. 1 Maja 1a | 169/2, 170/1 obręb Pozezdrze |
| 25 | Gmina Pozezdrze | Boisko Orlik | 11-610 Pozezdrze, ul. Pocztowa 5 | 2/2 obręb Pozezdrze |
| 26 | Gmina Pozezdrze | Budynek OSP Kuty | 11-610 Pozezdrze, Kuty 28 | 133 obręb Kuty |
| 27 | Gmina Pozezdrze | Budynek OSP Harsz | 11-610 Pozezdrze, Harsz 26b | 108 obręb Harsz |
| 28 | Gmina Orzysz | Urząd Miejski | 12-250 Orzysz, ul. Giżycka 15 | 293/4 obręb Orzysz |
| 29 | Gmina Orzysz | MOSiR Orzysz | 12-250 Orzysz, os. Robotnicze 14A | 21/10 obręb Orzysz |
| 30 | Gmina Orzysz | Centrum Informacji Turystycznej | 12-250 Orzysz, Rynek 5 | 89/9 obręb Orzysz |
| 31 | Gmina Orzysz | Park Jordanowski | 12-250 Orzysz, ul. Cierniaka | 249 obręb Orzysz |
| 32 | Gmina Orzysz | Plaża miejska | 12-250 Orzysz, ul. Leśna | 160/3 obręb Orzysz |
| 33 | Gmina Orzysz | Stadion miejski | 12-250 Orzysz, ul. 1 Maja | 155 obręb Orzysz |
| 34 | Gmina Orzysz | Biblioteka miejska | 12-250 Orzysz, ul. Wojska Polskiego 5 | 250/20 obręb Orzysz |
| 35 | Gmina Orzysz | Środowiskowy Dom Pomocy | 12-250 Orzysz, ul. Wojska Polskiego 17B | 411/43 obręb Orzysz |
| 36 | Gmina Orzysz | Świetlica wiejska | 12-250 Orzysz, Wierzbiny | 51/2 obręb Wierzbiny |
| 37 | Gmina Orzysz | Świetlica wiejska | 12-250 Orzysz, Ogródek 21 | 154/1 obręb Ogródek |
| 38 | Gmina Giżycko | Urząd gminy | 11-500 Giżycko, ul. Mickiewicza 33 | 484/6 obręb 2 |
| 39 | Gmina Giżycko | Urząd gminy | 11-500 Giżycko, ul. Mickiewicza 33 | 484/6 obręb 2 |
| 40 | Gmina Giżycko | Urząd gminy | 11-500 Giżycko, ul. Mickiewicza 33 | 484/6 obręb 2 |
| 41 | Gmina Giżycko | Urząd gminy | 11-500 Giżycko, ul. Mickiewicza 33 | 484/6 obręb 2 |
| 42 | Gmina Giżycko | Urząd gminy | 11-500 Giżycko, ul. Mickiewicza 33 | 484/6 obręb 2 |
| 43 | Gmina Giżycko | Urząd gminy | 11-500 Giżycko, ul. Mickiewicza 33 | 484/6 obręb 2 |
| 44 | Gmina Mikołajki | Biblioteka w Woźnicach | 11-730 Mikołajki, Woźnice 11a | 58 obręb Woźnice |
| 45 | Gmina Mikołajki | Biblioteka w Olszewie | 11-730 Mikołajki, Olszewo 20 | 80 obręb Olszewo |
| 46 | Gmina Mikołajki | Biblioteka miejska | 11-730 Mikołajki, ul. Kolejowa 6 | 219/8 obręb Mikołajki |
| 47 | Gmina Mikołajki | Urząd Miasta i Gminy | 11-730 Mikołajki, ul. Kolejowa 7 | 184/46 obręb Mikołajki |
| 48 | Gmina Mikołajki | Biblioteka w Baranowie | 11-730 Mikołajki, Baranowo 29 | 73/1 obręb Baranowo |
| 49 | Gmina Mikołajki | Rynek miasta | 11-730 Mikołajki, ul. Kolejowa 6 | 200/5 obręb Mikołajki |
| 50 | Gmina Mikołajki | Deptak nad jeziorem Mikołajskim przy MKŻ | 11-730 Mikołajki, ul. M. Kajki 84 | 439/6 obręb Mikołajki |
| 51 | Gmina Mikołajki | Nabrzeże portowe | 11-730 Mikołajki, ul. Kowalska 3 | 204 obręb Mikołajki |
| 52 | Gmina Mikołajki | Przystanek autobusowy | 11-730 Mikołajki, Plac Kościelny 3 | 192/1 obręb Mikołajki |
| 53 | Gmina Mikołajki | Hala sportowa | 11-730 Mikołajki, ul. Papieża Jana Pawła II 7 | 348/41 obręb Mikołajki |

### Wymagania minimalne punktów dostępowych

Tabela 19 Wymagania minimalne dotyczące parametrów punktów WiFi

|  |  |
| --- | --- |
| Lp. | Opis wymogu |
| 1. | Punkt dostępowy musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania na zewnątrz budynku [klasa min. IP67 – dotyczy jedynie punktów instalowanych na zewnątrz budynku]. Wymagane jest dostarczenie z punktami zestawu montażowego wraz z przewodami i patchcordami, zasilaczami, antenami i innymi akcesoriami wymaganymi do uruchomienia i prawidłowego działania systemu. |
| 2. | Wymagane parametry fizyczne:   1. Ethernet Interface 2. Zasilanie PoE (IEEE 802.3at PD) [może być realizowane przez dedykowany zasilacz PoE] 3. Slot karty SIM z modułem pracującym w standardzie LTE/4G 4. Temperatura pracy min. od -40 do +60 °C – jedynie w przypadku urządzeń instalowanych na zewnątrz, 5. Obudowa fabrycznie przystosowana do montażu na zewnątrz budynku [ściana i uchwyt] – jedynie w przypadku urządzeń instalowanych na zewnątrz. |
| 3. | Punkt musi obsługiwać co najmniej:   1. Standardy IEEE 802.11 a/b/g/n/ac 2. Jednoczesną pracę w standardach 802.11ac/n/a (5GHz) i 802.11n/g/b (2.4GHz) 3. do 1700Mbps przy 5GHz 4. do 300Mbps przy 2.4GHz 5. 64/128 bits WEP supported for encryption 6. Standardy zabezpieczeń: WPA-PSK, WPA2 PSK, Mixed WPA/WAP2 PSK 7. Tryby pracy: AP i WDS 8. Multiple SSID (min. 2 x SSID), BSSID 9. Wireless MAC Filtering 10. Wireless Client Isolation 11. Wi-Fi Hotspot z Captive Portal 12. Autentykacja RADIUS 13. limitowanie użycia łącza przez pojedynczego klienta wifi |
| 4. | Punkt musi posiadać wbudowany Firewall obsługujący min:   1. NAT firewall 2. Stateful Packet Inspection (SPI) 3. Zabezpieczenie przed DoS oraz Land Attack, Ping of Death, etc. 4. Access Control 5. IP Filtering, MAC Filtering, URL Filtering 6. VPN pass-through |
| 5. | Punkt musi obsługiwać protokoły i funkcje sieciowe min. w zakresie:   1. IPv4 2. NAT, Static Routing and RIP-1/2 3. SNTP, DNS relay and DDNS 4. IGMP Snooping and IGMP Proxy 5. DHCP server/client 6. Transparent Bridging 7. Network Time Protocol (NTP) 8. Monitorowania Syslog |
| 6. | Punkt musi zapewniać obsługę poprzez przeglądarkowy GUI, umożliwiać za jego pomocą upgrade Firmware, pobieranie i wysyłanie konfiguracji. Zarządzanie musi być możliwe również poprzez SNMP. |
| 7. | Urządzenie musi być przeznaczone na rynek Unii Europejskiej a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski. |
| 8. | Zamawiający wymaga, aby dostarczone urządzenie posiadało gwarancję minimum 2 lata, świadczoną przez Wykonawcę. Wymiana uszkodzonego elementu w trybie zgodnym z SLA dla Projektu. Okres gwarancji liczony będzie od daty sporządzenia protokołu przekazania przedmiotu zamówienia. |
| 9. | Zamawiający wymaga aby przez cały okres gwarancji wszelkie aktualizacje oprogramowania były bezpłatne. |
| 10. | Zamawiający wymaga aby do każdego punktu WiFi dostarczone zostały karty SIM zezwalające na nielimitowany dostęp do internetu za pomocą technologii LTE w okresie trwałości projektu. |
| 11. | Zamawiający wymaga dostarczenia pełnej dokumentacji pozwalającej pracownikom Centrum Kompetencji zarządzać zdalnie bezprzewodowymi punktami dostępu WiFi. |
| 12 | Zarządzanie punktami może się odbywać się za pośrednictwem dedykowanej konsoli. |

# Zakres 2. Dostawa Systemów EOD, Szyn Danych lokalnych i centralnej wraz z zestawem konektorów oraz Portalu Usług Elektronicznych

## System EOD (EZD PUW)

EZD PUW – pozyskanie i wdrożenie systemu nie jest przedmiotem zamówienia. Zamieszczona dokumentacja interfejsu EZD służy jedynie zdefiniowaniu parametrów i zasad wymiany danych pomiędzy portalem E-usług i systemem EZD PUW.

Dokumentacja niezbędna do tego celu stanowi Załącznik nr 8 do SIWZ.

## Usługi udostępnione dla poziomu centralnego

W celu dostarczenia zaawansowanych usług elektronicznych dla mieszkańców i przedsiębiorców obszaru Wielkich Jezior Mazurskich konieczne jest dostarczenie usług integracji EOD i SD na potrzeby Portalu Usług Elektronicznych.

Integracja ta ma na celu udostępnienie aktualnych informacji podatkowych (należności, płatności) oraz stan spraw urzędowych dla SUE. Integracja będzie możliwa do realizacji, o ile system EOD (PUW) będzie posiadał dostarczone interfejsy integracyjny w opisanym zakresie. W przypadku, kiedy PUW nie będzie posiadał poniższych możliwości integracyjnych, wówczas Wykonawca uzgodni dostarczenie integracji w momencie technicznej możliwości udostępnionej przez PUW w okresie gwarancji projektu.

## Wdrożenie EOD, integracji

Wdrożenie ma na celu przeprowadzenie procesu umożliwiającego każdemu z partnerów korzystanie z lokalnej infrastruktury systemowej.

Wykonawca musi działać w oparciu o system zarządzania jakością zgodny z wymaganiami ISO 9001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny oraz w oparciu o system zarządzania jakością zgodny z wymaganiami ISO/IEC 27001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny.

Tabela 21 Zakres prac w ramach wdrożenia EOD i integracji

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WW1 | Wykonawca ma obowiązek przeprowadzenia analizy przedwdrożeniowej obejmującej:  - analizę dotychczasowego sposobu organizacji pracy w obszarach Systemów Dziedzinowych i EZD  - analiza bezpieczeństwa transmisji danych pomiędzy systemami EZD, i centralnym SUE. |
| WW2 | Wykonawca ma obowiązek uzgodnienia z Zamawiającym Planu wdrożenia obejmującego:  - listę wymaganych czynności wykonywanych po stronie Zamawiającego  - uzgodnienie sposobu odbioru procesu wdrożenia EZD, i integracji |
| WW3 | W ramach usług wdrożeniowych, Wykonawca zrealizuje:   * Udostępnienie na infrastrukturze sprzętowej Partnera systemu EZD na potrzeby procesu wdrożenia i szkolenia * Skonfiguruje warstwę sprzętową, systemową i sieciową gwarantując odpowiedni poziom bezpieczeństwa * Uzgodni i wdroży poziom bezpieczeństwa w obszarze integracji z systemami partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020. |

# Zakres 3. Dostarczenie i wdrożenie formularzy elektronicznych

Wykonawca dokona pełnego wdrożenia formularzy elektronicznych na ePUAP w Środowisku Budowy Aplikacji.

Tabela 22 Parametry minimalne wdrożonych formularzy elektronicznych

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WF1 | Formularze stosowane na ePUAP tworzone są z wykorzystaniem języka XForms oraz XPath. |
| WF2 | Wykonawca opracuje formularze elektroniczne (zgodnie z właściwymi przepisami prawa) na podstawie przekazanych przez JST, których dotyczy przedmiotowe zamówienie, kart usług z formularzami w formacie MS Word. |
| WF3 | Wszystkie formularze elektroniczne Wykonawca przygotuje z należytą starannością tak, aby pola do uzupełnienia w tych formularzach zgadzały się z polami formularzy w formacie MS Word. |
| WF4 | Pola wskazane przez JST jako pola obowiązkowe w formularzach w formacie MS Word, musza zostać polami obowiązkowymi również w formularzach elektronicznych. |
| WF5 | Układ graficzny wszystkich formularzy powinien być w miarę możliwości jednolity. |
| WF6 | Wizualizacja formularzy elektronicznych nie musi być identyczna ze wzorem w formacie MS Word, ale musi zawierać dane w układzie niepozostawiającym wątpliwości co do treści i kontekstu zapisanych informacji, w sposób zgodny ze wzorem oraz obowiązującymi przepisami prawa. |
| WF7 | Przygotowując formularze Wykonawca musi dążyć do maksymalnego wykorzystania słowników. |
| WF8 | W budowanych formularzach należy wykorzystać mechanizm automatycznego pobierania danych z profilu – celem uzupełnienia danych o wnioskodawcy. |
| WF9 | Formularze muszą zapewniać walidację wprowadzonych danych po stronie klienta i serwera zgodnie z walidacją zawartą w schemacie dokumentu. |
| WF10 | Jeśli w formularzu elektronicznym występują pola PESEL, REGON lub kod pocztowy, to pola te muszą być walidowane pod kątem poprawności danych wprowadzanych przez wnioskodawcę. |
| WF11 | Każdy opracowany przez Wykonawcę formularz (w postaci pliku XML) musi zostać przekazany JST na okres 7 dni roboczych w celu dokonania sprawdzenia i wykonania testów na formularzu. |
| WF12 | Po okresie testów, o których mowa w wymaganiu poprzednim, JST przekaże Wykonawcy ewentualne poprawki i uwagi dotyczące poszczególnych formularzy, które Wykonawca usunie bez zbędnej zwłoki. |
| WF13 | Wykonawca przygotuje wzory dokumentów elektronicznych w CRD zgodnie ze standardem ePUAP w formacie XML zgodnym z formatem Centralnego Repozytorium Wzorów Dokumentów. |
| WF14 | Zamawiający dopuszcza możliwość wykorzystania przez Wykonawcę wzorów, które są już opublikowane w CRD. |
| WF15 | Wygenerowane dla poszczególnych formularzy wzory dokumentów elektronicznych, składające się z plików:   * Wyróżnik (wyróżnik.xml) * Schemat (schemat.xml) * Wizualizacja (styl.xsl)   muszą zostać dostosowane do wymogów formatu dokumentów publikowanych w CRD i spełniać założenia interoperacyjności. |
| WF16 | W ramach projektu Wykonawca przygotuje i przekaże Zamawiającemu wszystkie wzory dokumentów elektronicznych w celu złożenia wniosków o ich publikację w CRD. |
| WF17 | Wykonawca udzieli wsparcia Zamawiającemu w przejściu procesu publikacji na ePUAP. |
| WF18 | Bazując na przygotowanych wzorach dokumentów elektronicznych oraz opracowanych na platformie ePUAP formularzach elektronicznych Wykonawca przygotuje instalacje aplikacji w środowisku ePUAP. |
| WF19 | Aplikacje muszą być zgodne z architekturą biznesową ePUAP oraz architekturą systemu informatycznego ePUAP. |
| WF20 | Przygotowane aplikacje muszą zostać zainstalowane przez Wykonawcę na koncie ePUAP Zamawiającego. |
| WF21 | Zainstalowane aplikacje muszą spełniać wymogi ePUAP oraz pozytywnie przechodzić przeprowadzone na ePUAP walidacje zgodności ze wzorami dokumentów. |
| WF22 | Na czas realizacji projektu Zamawiający zapewni Wykonawcy dostęp do części administracyjnej platformy ePUAP konta JST z uprawnieniami do konsoli administracyjnej Draco, ŚBA i usług. |
| WF23 | W przypadku zwłoki w publikacji wzorów dokumentów CRD realizowanej przez Ministerstwo Cyfryzacji (administrator ePUAP) dopuszcza się dokonanie odbioru tej części zamówienia w ramach lokalnych publikacji w CRD z zastrzeżeniem, że Wykonawca dokona przekonfigurowania aplikacji po pomyślnej publikacji CRD przez Ministerstwo Cyfryzacji. |
| WF24 | Zamawiający przekaże Wykonawcy opisy usług w formacie MS Word. |
| WF25 | Zamawiający dopuszcza, aby Wykonawca wykorzystał opisy usług umieszczone na platformie ePUAP. |
| WF26 | Zadaniem wykonawcy jest odpowiednie powiązanie opisów usług zamieszczonych na ePUAP z odpowiednimi usługami opracowanymi przez JST. |
| WF27 | Wykonawca przygotuje definicję brakujących opisów usług na ePUAP. Zamawiający zwróci się do Ministerstwa Cyfryzacji w celu akceptacji i umieszczenia ich na platformie ePUAP. |
| WF28 | Wszystkie opisy usług zostaną przyporządkowane do jednego lub więcej zdarzenia życiowego z Klasyfikacji Zdarzeń, a także do Klasyfikacji Przedmiotowej Usług ePUAP. |

Zadaniem Wykonawcy jest dostarczenie formularzy dla Partnerów projektu, wg. Poniższego zapotrzebowania. O ile prawo centralne lub lokalnej nie wymaga inaczej, Wykonawca może zaproponować wspólne wzory i formularze dokumentów dla tych samych usług poszczególnym partnerom projektu.

Tabela 23 Lista formularzy elektronicznych wdrażanych u poszczególnych Partnerów Projektu

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | rodzaj dokumentu  W- wniosek, Z- zgłoszenie | Nazwa | Podmioty objęte dostawą |
| 1. | W | Udostępnienie informacji ze zbioru danych osobowych | Wszyscy partnerzy (12 szt.) |
| 2. | W | Dostęp do informacji publicznej | Wszyscy partnerzy (12 szt.) |
| 3. | Z | Rozpatrywanie skarg i wniosków | Wszyscy partnerzy (12 szt.) |
| 4. | W | Wydawanie zaświadczeń | Wszyscy partnerzy (12 szt.) |
| 5. | W | Rozpatrywanie petycji | Wszyscy partnerzy (12 szt.) |
| 6. | W | Uzyskanie dofinansowania do kosztów usuwania azbestu | Gminy (11 szt.) |
| 7. | W | Zezwolenie na sprzedaż napojów alkoholowych | Gminy (11 szt.) |
| 8. | W | Wydanie odpisu danych z rejestru dowodów osobistych | Gminy (11 szt.) |
| 9. | W | Wydanie odpisu danych z rejestru mieszkańców i cudzoziemców | Gminy (11 szt.) |
| 10. | W | Sprawy związane z miejscowym planem zagospodarowania przestrzennego - wniosek o wydanie zaświadczenia o przeznaczeniu w miejscowym planie zagospodarowania przestrzennego | Gminy (11 szt.) |
| 11. | W | Wydanie decyzji o ustaleniu warunków zabudowy lub lokalizacji inwestycji celu publicznego | Gminy (11 szt.) |
| 12. | W | Wydanie pozwolenia na budowę, rozbiórkę lub przeniesienie decyzji o pozwoleniu na budowę na rzecz innej osoby | Starostwo (1 szt.) |
| 13. | W | Wydanie decyzji pozwolenia na zmianę sposobu użytkowania obiektu budowlanego | Starostwo (1 szt.) |
| 14. | Z | Przyjęcie zgłoszenia zamiaru wykonania robót budowalnych niewymagających pozwolenia | Starostwo (1 szt.) |
| 15. | W | Wydanie wypisów i wyrysów oraz zaświadczenia z operatu ewidencyjnego | Starostwo (1 szt.) |
| 16. | W | Koordynacja dokumentacji projektowej sieci uzbrojenia terenu | Starostwo (1 szt.) |
| 17. | W | Udostępnienie kopii materiałów geodezyjnych i kartograficznych | Starostwo (1 szt.) |
| 18. | W | Udostępnienie rzeczoznawcom majątkowym danych o nieruchomościach | Starostwo (1 szt.) |
| 19. | W | Rejestracja lub skreślenia w Ewidencji Starosty stowarzyszenia zwykłego | Starostwo (1 szt.) |
| 20. | W | Wydanie pozwoleń na sprowadzenie do Polski zwłok lub szczątków osób zmarłych za granica | Starostwo (1 szt.) |
| 21. | W | Opiniowanie projektów studium uwarunkowań | Starostwo (1 szt.) |
| 22. | W | Uzgadnianie planów zagospodarowania przestrzennego | Starostwo (1 szt.) |
| 23. | Z | Ochrona przed bezdomnymi zwierzętami | Gminy (11 szt.) |
| 24. | W | Prowadzenie schronisk dla bezdomnych zwierząt | Gminy (11 szt.) |
| 25. | W | Deklaracja o wysokości opłaty za gospodarowanie odpadami komunalnymi dla nieruchomości zamieszkałych i niezamieszkałych | Gminy (11 szt.) |
| 26. | W | Wpis do rejestru działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości | Gminy (11 szt.) |
| 27 | W | Udzielanie zezwolenia na świadczenie usług w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych | Gminy (11 szt.) |
| 28 | W | Uzyskanie zezwolenia na usunięcie drzewa | Gminy (11 szt.) |
| 29 | W | Wydanie decyzji o środowiskowych uwarunkowaniach zgody na realizację przedsięwzięcia | Gminy (11 szt.) |
| 30 | W | Obszar wyznaczony do rewitalizacji | Gminy (11 szt.) |

Razem 225 formularzy dla dokumentów elektronicznych.

# Zakres 4. Wdrożenie Portalu Usług Elektronicznych oraz zapewnienie bezpieczeństwa transmisji danych.

System centralnych Usług Elektronicznych umożliwi Zamawiającemu realizacje głównych celów projektu. SUE będzie odpowiedzialna za dostarczenie elektronicznych usług na poziomie 4-transkacja i 3- dwustronna interakcja. Będzie odpowiadał za poprawę formy kontaktu z klientem JST obszaru Wielkich Jezior Mazurskich.

PUE umożliwi integrację z 12 lokalnymi środowiskami (szynami danych na poziomie JST) i tym samym zagwarantuje przepływ odpowiednich danych pomiędzy SUE a JST.

Dostarczany System Usług elektronicznych będzie **rozwiązaniem wysoko innowacyjnym** zarówno w regionie jak i w kraju. Rozwiązanie to zintegruje jednolitą informację podatkową, finansową i rozliczeniową dla klientów regionu Wielkich Jezior Mazurskich w ramach jednego portalu SUE.

## Warstwa administracji i integracji

System Usług Elektronicznych musi stanowić moduł całego systemu umożliwiający bezpośredni kontakt z partnerami Stowarzyszenia Wielkie Jeziora Mazurskie 2020. Będzie systemem udostępnionym w sieci Internet dla wszystkich potencjalnych odbiorców. System ten będzie zawierał warstwę publiczną (dostęp do opisu Kart Usług oraz Spraw Urzędowych), która będzie dostępna dla wszystkich użytkowników zewnętrznych.

Warstwa wymagająca autoryzacji systemu SUE będzie przeznaczona dla klientów JST do realizacji usług publicznych. Aby móc sprawdzić stan sprawy urzędowej, zapisać się na spotkanie w odpowiednim referacie odpowiedniego Partnera Stowarzyszenia Wielkie Jeziora Mazurskie 2020 lub zapłacić online np. za śmieci, klient JST będzie zobowiązany dokonać autoryzacji m.in. za pomocą profilu zaufanego.

System będzie posiadał także obszar administracyjny, przeznaczony dla pracowników urzędów. Obszar ten umożliwi skonfigurowanie SUE i połączenie konta klienta z odpowiednimi danymi pochodzącymi z systemów dziedzinowych oraz obiegu dokumentów.

Tabela 24 Parametry minimalne SUE

|  |  |
| --- | --- |
| KOD | Wymaganie |
| WSDW1 | System musi posiadać jedno logowanie przeznaczone dla wszystkich modułów. |
| WSDW2 | Użytkownik będzie mógł zalogować się do systemu za pomocą konta ePUAP.  Użytkownik musi być automatycznie zalogowany do systemu, o ile jest zalogowany do ePUAP. |
| WSDW3 | Użytkownik będzie mógł samodzielnie założyć konto w systemie nie posiadając konta na ePUAP. |
| WSDW4 | Użytkownik będzie mógł samodzielnie założyć konto w systemie posiadając konto na ePUAP. |
| WSDW5 | Użytkownik może korzystać z funkcji Przypomnij Hasło, która umożliwia mu samodzielne odzyskanie hasła do systemu.  Funkcja przypomnij hasło wymusza ponowne ustawienie hasła do systemu. |
| WSDW6 | System musi wymagać hasła na odpowiednim poziomie bezpieczeństwa, tzn. minimum 8 znaków, w tym przynajmniej jedna duża i mała litera oraz cyfra – zgodnie z ustawą o ochronie danych osobowych i z RODO |
| WSDW7 | System musi być zaprojektowany w architekturze trójwarstwowej. |
| WSDW8 | Warstwa danych musi być oparta o silnik bazy danych SQL umożliwiający instalację zarówno na systemie operacyjnym Windows jak i Linux. |
| WSDW9 | Warstwa serwera aplikacyjnego musi dostarczać logikę biznesową systemu i umożliwia instalację na systemie operacyjnym Windows i Linux. |
| WSDW10 | Warstwa prezentacyjna musi być dostosowana do przeglądarek internetowych w wersjach aktualnych na dzień składania zamówienia. |
| WSDW11 | System musi być dostosowany do dostępu dla osób niedowidzących, tj. zgodność z wymogami WCAG 2.0 na poziomie AA. |
| WSDW12 | System powinien umożliwiać rejestrację użytkowników:   * 1. zewnętrznych (interesantów partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020);   2. wewnętrznych (pracowników partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020) z oznaczeniem administratorów portalu, którzy posiadają rozszerzone uprawnienia m.in. do publikacji artykułów i aktualności oraz administrowania systemem. |
| WSDW13 | Rejestracja użytkownika musi wymagać podania jego loginu, hasła, imienia, nazwiska, daty urodzenia, adresu e-mail oraz opcjonalnie numeru telefonu (w celu otrzymywania powiadomień sms). Dodatkowo użytkownik musi wyrazić zgodę na przetwarzanie jego danych osobowych oraz potwierdzić zapoznanie się i akceptację regulaminu. |
| WSDW14 | Rejestracja użytkowników zewnętrznych musi być możliwa przy pomocy formularza, który może złożyć niezalogowany użytkownik. Taka rejestracja będzie wymagać akceptacji administratora systemu. |
| WSDW15 | Rejestracji użytkowników wewnętrznych musi dokonać administrator systemu w ramach funkcjonalności zarządzania użytkownikami. |
| WSDW16 | Ze względu na zakładany dostęp do systemu z poziomu urządzeń mobilnych, strony systemu powinny automatycznie dostosowywać się do różnych rozdzielczości ekranu (Responsive Web Design). |
| WSD1W7 | System w zakresie stron www musi być przygotowany zgodnie ze standardem W3C. |
| WSDW18 | Podstawowym językiem obowiązującym w systemie musi być język polski. |
| WSDW19 | Jeżeli system będzie korzystał z ciasteczek, wówczas na stronie głównej musi być prezentowana informacja o tym fakcie wraz z możliwością przeglądu polityki wykorzystania ciasteczek. |
| WSDW20 | System musi rejestrować operacje tworzenia, edycji i usuwania obiektów (ofert, zabytków, map itp.) wraz z informacją o użytkowniku, dacie i czasie wykonania operacji. Dodatkowo system musi udostępniać funkcjonalność do przeglądu zarejestrowanych operacji. |
| WSDW21 | Korzystanie z systemu przez użytkowników, oprócz przeglądarki Firefox, Chrome, Internet Explorer, Safari, które są zgodne ze standardem HTML 5, nie może wymagać instalacji dodatkowego oprogramowania |
| WSDW22 | Przy założeniu, że system będzie udostępniany użytkownikom zewnętrznym, którzy będą posiadać komputery o następujących parametrach minimalnych:  a. Procesor dwurdzeniowy;  b. Pamięć - 2 GB;  c. Łącze - 1Mb/s;  czas odpowiedzi serwera na wywołanie url aplikacji musi wynosić maksymalnie 3 sekundy. Powyższe założenie musi być spełnione przy 100 użytkownikach zalogowanych jednocześnie do systemu. Określony czas nie dotyczy wywołań systemów zewnętrznych. |
| WSDW23 | System powinien umożliwiać administratorowi systemu na określenie maksymalnej wielkości pobieranych plików oraz zdjęć. W przypadku zdjęć, których wielkość będzie przekraczać zakładaną wartość, system powinien informować o możliwościach zmiany tej wielkości (np. poprzez zwiększenie kompresji lub zmianę rozdzielczości). |
| WSDW24 | System musi umożliwiać administratorowi zarządzanie zadaniami wsadowymi przeznaczonymi do zadań administracyjnych wykonywanych automatycznie. W ramach zarządzania zadaniami wsadowymi administrator ma możliwość skonfigurowania planu wykonywania zadania wsadowego, parametrów jego wywoływania, przeglądu logów z wykonanych zadań wsadowych |
| WSDW25 | System musi umożliwiać zarządzanie przynajmniej następującymi zadaniami wsadowymi:   * czyszczenie katalogu plików, * weryfikacja stanu wiadomości SMS wysyłanych do użytkowników, * usuwanie wygenerowanych raportów z modułu raportowego, * wysyłanie powiadomień o należnościach. |
| WSDW26 | System musi umożliwiać zarządzanie rejestrem interesantów pochodzących od wszystkich partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020, gdzie każdego można:   * zidentyfikować minimum takimi danymi jak: typ podmiotu, Imię, Nazwisko, Login, zdjęcie profilowe, dane kontaktowe (telefon, e-mail, faks, www, adres korespondencyjny, oraz dowolną liczbę innych form kontaktu), * zmienić mu dane podstawowe, * zmienić mu dane kontaktowe, * powiązać go z interesantem z wybranego systemu dziedzinowego, * aktywować konto interesanta, * przypisać interesanta do grup użytkowników. |
| WSDW27 | Ilekroć w systemie jest możliwość dodania dokumentu, zdjęcia lub innego pliku system musi umożliwiać skorzystanie z funkcji Drag-and-Drop i umożliwia „przeniesienie pliku” z katalogu użytkownika komputera. |
| WSDW28 | Ilekroć w systemie jest mowa o danych ze słownika TERYT, system musi prezentować listę rozwijalną z aktualnych danych TERYT. |
| WSDW29 | System musi umożliwiać zarządzania słownikiem TERYT z możliwością importu pliku w opcjach: Miejscowości, Podział terytorialny, Nazwy ulic. |
| WSDW30 | Ilekroć w systemie wykorzystywany jest element słownika TERYT, system musi prezentować pole automatycznie przeszukiwane wielotekstowo według znaków wprowadzanych przez użytkownika. Prezentowana lista musi zawierać w każdym wierszu kilka najistotniejszych elementów m.in. Nazwę województwa, powiatu i gminy – w przypadku wyszukiwania miejscowości. |
| WSDW31 | System musi posiadać wydzieloną funkcję umożliwiającą przeglądnie Interesantów do aktywacji i aktywowanie im kont. |
| WSDW32 | System musi umożliwiać zmianę hasła dla zalogowanego użytkownika. |
| WSDW33 | System musi umożliwiać zarządzanie odrębnym rejestrem pracowników, w którym każdy pracownik charakteryzowany jest za pomocą Imienia, Nazwiska (z opcją dodania 2 i 3 członu nazwiska), Symbolu (skrótu pracownika), Stanowiska pracownika, loginu, zdjęcia profilowego, danych kontaktowych (telefon, e-mail, lokalizacja, faks, www, adresu korespondencyjnego, lub jakiejkolwiek innego kontaktu z rozróżnieniem formy tego kontaktu) |
| WSDW34 | Zarówno dla interesanta jak i pracownika system musi umożliwiać przeglądanie rejestru czynności wykonywanych przez wybranego użytkownika z wyróżnieniem daty i czasu wykonania czynności oraz obiektu w systemie, którego to dotyczy. |
| WSDW35 | System musi posiadać możliwość zarządzania słownikiem kodów pocztowych wraz z importem kodów pocztowych z pliku CSV Poczty Polskiej. |
| WSDW36 | System musi posiadać możliwość edycji głównych stron każdego z modułów. Edycja głównej strony modułu umożliwia, co najmniej:   * ustalenie stylu redagowanego tekstu * Pogrubienie, podkreślenie, pochylenie tekstu, * Wyczyszczenie formatu czcionki, * Ustalenie kolor czcionki, * Ustalenie sposobu punktowania, * Ustalanie wielkości odstępów pomiędzy liniami tekstu, * Dodanie obrazka, * Dodanie linka do innej strony, * Wstawienie tabeli, * Przegląd redagowanej treści w formie HTML. |
| WSDW37 | System musi umożliwiać zarządzanie rolami w systemie, przy czym system w ramach dostarczenie posiada przygotowane podstawowe role do każdego z modułów systemu. |
| WSDW38 | Każda z ról systemu musi posiadać listę uprawnień wraz z opisami uprawnień. |
| WSDW39 | Administrator musi mieć możliwość dodania dowolnej roli w systemie i przypisania jej dowolnej listy uprawnień. |
| WSDW40 | System ról, uprawnień i użytkowników musi być oparty o mechanizmy LDAP. |
| WSDW41 | System ról, uprawnień i użytkowników musi posiadać interfejs użytkownika w ramach SUE, który umożliwia ergonomiczne i efektywne zarządzanie tym zakresem. |
| WSDW42 | System musi posiadać funkcję „przeładowania uprawnień” w trybie rzeczywistym systemu. Przeładowanie uprawnień wymianie listy uprawnień na serwerze aplikacyjnym, co pozwala na zarządzanie dostępami bez konieczności wylogowywania użytkowników systemu. |
| WSDW43 | System musi posiadać funkcję zarządzania rolami przypisanymi do użytkowników. |
| WSDW44 | System musi posiadać miejsce do zarządzania wszelką parametryzacją systemu, gdzie:   * Pogrupowane są obszary parametryzacji systemu, * Każdy z parametrów posiada funkcję edycji, * Każdy z parametrów charakteryzowany jest przez opis, nazwę i wartość. |
| WSDW45 | System musi być sparametryzowany m.in. w zakresie: obsługi e-mail, LDAP, płatności elektronicznych, danych JST integrowanych systemów, danych dostępowych do ePUAP. |
| WSDW46 | System musi posiadać obszar zarządzania plikami zaimportowanymi do systemu na potrzeby udostępniania w innych modułach. |
| WSDW47 | System musi posiadać możliwość przeglądania rejestru operacji wykonanych w systemie. Przegląd rejestru operacji możliwy jest do przeszukania m.in. według daty i czas od – do, użytkownika, który dokonał operacji, typu obiektu i rodzaju operacji wykonywanej (np. aktualizacja danych, błąd, modyfikacja danych, usunięcie danych, import, etc.). |
| WSDW48 | System musi mieć możliwość zarządzania strukturą organizacyjną Stowarzyszenia Wielkie Jeziora Mazurskie 2020 w formie prezentacji jako drzewo organizacji, które wyróżnia: Komórkę Organizacyjną, Stanowisko oraz Pracownika na stanowisku. |
| WSDW49 | SUE w warstwie publicznej będzie udostępniony wyłącznie za pośrednictwem aplikacji udostępnionej na serwerze www dostosowanej do przeglądania zarówno na komputerach przenośnych jak i na urządzeniach mobilnych z uwzględnieniem Responsive Design. |

## Moduł konta klienta

Moduł konta klienta musi umożliwiać zarządzanie i przeglądanie danych zautoryzowanego użytkownika oraz użytkownika powiązanego z kontrahentami z systemów dziedzinowych partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020.

Tabela 25 Parametry minimalne modułu konta klienta

|  |  |
| --- | --- |
| KOD | Wymaganie |
| WSKK1 | Użytkownik zalogowany do systemu musi mieć możliwość przeglądania i zmiany własnych danych:   * Typ podmiotu (podmiot, osoba fizyczna), * Imię, * Nazwisko / nazwa, * Dane kontaktowe standardowe: telefon, email, fax, www, adres korespondencyjny * Dane kontaktowe dodatkowe. |
| WSKK2 | Użytkownik musi mieć możliwość zmiany hasła. |
| WSKK3 | Użytkownik musi mieć możliwość powiązania kont z kontem ePUAP. |
| WSKK4 | Użytkownik musi mieć możliwość odłączenia konta od ePUAP. |
| WSKK5 | Użytkownik musi mieć możliwość przeglądu danych kontrahent z systemu dziedzinowego, o ile jego konto zostało powiązane z kontem kontrahenta systemu dziedzinowego. |
| WSKK6 | Dane podstawowe prezentowane w przypadku powiązania konta z kontrahentem z wybranego SD to co najmniej: Nazwisko Imię / Nazwa, Typ, PESEL, NIP, Data wyrejestrowania lub zgonu (jeśli widnienie w SD). |
| WSKK7 | O ile konto powiązane jest z SD odpowiedniego partnera Stowarzyszenia Wielkie Jeziora Mazurskie 2020, system musi prezentować:   * Dane zameldowania, o ile użytkownik jest zameldowany na terenie JST, * Listę nieruchomości, gdzie dla każdej nieruchomości prezentowana jest nazwa gminy, wielkość, typ nieruchomości, typ własności lista opłat i podatków pobieranych z tytułu nieruchomości: m.in.: podatek od osób fizycznych, podatek od osób prawnych, opłaty za śmieci, * Listę dzieci, o ile zalogowany użytkownik jest osobą fizyczną posiadającą dzieci do lat 18 zameldowane w tym samym gospodarstwie domowym, * Listę środków transportu – podlegającą opłatom o ile SD użytkownik jest podmiotem prawnym posiadającym opodatkowane środki transportu, lista środków transportu będzie posiadała wskazanie na gminę, z której została pobrana. * Listę aktualnych zezwoleń na sprzedaż napojów alkoholowych, o ile zalogowany użytkownik jest podmiotem prawnym. Lista zezwoleń będzie wskazywała Gminę, na terenie której zostało wydane dane zezwolenie. * Listę psów   Wszystkie dane muszą być pobierane z systemów SD i EOD, o ile dane JST prowadzi wskazane rejestry. |
| WSKK8 | Administrator musi mieć możliwość powiązania użytkownika z wieloma kontami kontrahentów Systemów Dziedzinowych zintegrowanych, z założeniem, że może istnieć tylko jedno wskazanie dla danego zintegrowanego systemu dziedzinowego (w rozumieniu jeden system dziedzinowy to jeden podmiot Stowarzyszenia Wielkie Jeziora Mazurskie 2020). |
| WSKK9 | Moduł konta klienta w zakresie informacji prezentowanych dla mieszkańca, obywatela czy przedsiębiorcy zostanie dostarczony w ramach aplikacji www. |

## Moduł elektronicznego biura interesanta

Moduł elektronicznego biura interesanta będzie stanowił wirtualny punkt przyjęć formularzy elektronicznych stosowanych w urzędach Stowarzyszenia Wielkie Jeziora Mazurskie 2020 oraz informacji dotyczących sposobu załatwienia każdej sprawy, którą można zrealizować w urzędzie.

Moduł musi być podzielny na część publiczną – udostępnianą niezalogowanym użytkownikom oraz część wewnętrzną – dla administratora systemu. Część ta prezentuje uprzednio zredagowane karty usług spraw urzędowych świadczonych przez jednostki samorządu Stowarzyszenia Wielkie Jeziora Mazurskie 2020.

Tabela 26 Wymagania minimalne dot. modułu elektronicznego biura interesanta

|  |  |
| --- | --- |
| KOD | Wymaganie |
| WSBI1 | Moduł musi posiadać stronę główną umożliwiającą dodanie nazwy adresu, znaku graficznego Stowarzyszenia Wielkie Jeziora Mazurskie 2020, ustawienie głównych funkcji, do których szybko mogą dotrzeć użytkownicy portalu. |
| WSBI2 | Moduł w części publicznej musi prezentować pokategoryzowane karty usług pod kątem życiowych zdarzeń, wydziałów i innych dodatkowych klasyfikacji oraz JST Stowarzyszenia Wielkich jezior Mazurskich 2020. |
| WSBI3 | Użytkownik w części publicznej powinien mieć możliwość przejrzenia karty usługi, dla której prezentowanej jest:   * Opis zredagowany przez administratora, * Dostępne terminy wizyt w wybranym urzędzie, * Zarezerwowania terminu wizyty w wybranym urzędzie, * Przejścia do wypełnienia formularza elektronicznego na ePUAP. |
| WSBI4 | Kart usługi powinna być charakteryzowana przynajmniej przez następujące atrybuty: nazwę, opis, do kogo jest skierowana (obywatel- czyli usługi typu A2C, przedsiębiorcy -czyli usługi typu A2B, instytucji/urzędu – czyli usługi typu A2A), liczba czasu obsługi klienta przy okienku dla danego rodzaju sprawy, kategorię (np. Budownictwo i Nieruchomości, Ochrona środowiska etc.). Administrator ma możliwość zdefiniowania karty usługi dla danego urzędu Stowarzyszenia Wielkie Jeziora Mazurskie 2020. |
| WSBI5 | Administrator musi mieć możliwość utworzenia wizualizacji karty usług. |
| WSBI6 | W przypadku publikowania karty usługi, administrator musi być zobowiązany do podania daty, od kiedy publikacja obowiązuje oraz powodu publikacji. |
| WSBI7 | W przypadku zmiana opisu karty usługi, administrator musi być zobowiązany do podania powodu zmiany wizualizacji karty usługi. |
| WSBI8 | W przypadku zdejmowania z publikacji kary usługi, administrator musi być zobowiązany do podania powodu zdjęcia z publikacji karty usługi. |
| WSBI9 | Dla każdej usługi wybrany urząd musi mieć możliwość określenia dni i godziny dyżurów, w których pracownik gminy jest w stanie pomóc mieszkańcom lub odpowiadać na pytania w danym zakresie. |
| WSBI10 | Obsługa dyżurów powinna obejmować obejmuje: ustalenie dyżuru w zakresie (karty usługi lub kilku kart usług, której dotyczy, daty od, okienka godzinnego od – do), ma możliwość ustalenia przerwy w trakcie dyżuru. Podczas dodawania dyżuru użytkownik musi mieć możliwość wykonania automatycznej funkcji ustalenia analogicznego dyżuru powielonego w następnym tygodniu lub miesiącu. |
| WSBI11 | Administrator po dodaniu dyżuru musi mieć możliwość ustalenia jego publikacji ze wskazaniem daty obowiązywania od. |
| WSBI12 | W przypadku zmiany ustawień dyżuru, usunięcia lub zdjęcia z publikacji administrator musi być zobowiązany do podania powodu zmiany. |
| WSBI13 | Pracownicy obsługujący dyżury powinni mieć możliwość przejrzenia grafiku dyżurów wraz z listą osób zapisanych na spotkanie, w szczególności danych: imię, nazwisko, PESEL, e-mail, telefon. |
| WSBI14 | Zapisania na dyżur powinien móc dokonać zarówno użytkownik zarejestrowany w systemie jak i niezarejestrowany. |
| WSBI15 | W przypadku zapisania na spotkanie użytkownika zarejestrowanego, system musi automatycznie podpowiadać dane z karty użytkownika. |
| WSBI16 | Użytkownik musi otrzymać mailem informację w celu potwierdzenia spotkania. |
| WSBI17 | Moduł elektronicznego biura interesanta w zakresie informacji skierowanych do mieszkańca i przedsiębiorcy (karty spraw i usług, połączone formularze, zapisywanie na wizytę) zostanie dostarczony w ramach aplikacji www. |

## Moduł płatności online

Platforma dająca mieszkańcom (dzięki integracji z Systemami Dziedzinowymi) z partnerów Stowarzyszenia Wielkie Jeziora Mazurskie 2020 wgląd w stan ich rozliczeń z urzędem, zintegrowana z systemami bankowymi, oraz musi umożliwiać uregulowanie należności online.

Dostęp do danych płatnościowych będzie możliwy wyłącznie dla zarejestrowanych użytkowników systemu SUE dodatkowo posiadających konto powiązane z kontrahentem przynajmniej jednego Systemu Dziedzinowego Stowarzyszenia.

Tabela 27 Wymagania minimalne dot. modułu Płatności 0n-line

|  |  |
| --- | --- |
| KOD | Wymaganie |
| WSPŁ1 | Po zalogowaniu na swoje konto obywatel lub przedsiębiorca powinien zobaczyć wszystkie swoje należności wobec JST Stowarzyszenia Wielkie Jeziora Mazurskie 2020 pobrane z SD niezależnie od tytułu (podatki, opłaty lokalne, opłaty za śmieci, umowy dzierżawy itp.), które są wystawiane w modułach dziedzinowych, oraz historię jego płatności. Będzie to przegląd wszystkich zobowiązań finansowych z uwzględnieniem tytułu należności, należności głównej (w tym Vat – jeśli wymagany), odsetki, koszty upomnień, wezwań do zapłaty, salda do zapłaty, terminie płatności, kwocie już zapłaconej (w przypadku należności, która została już częściowo spłacona), kwocie zleconej płatności poprzez portal oraz dacie i godzinie zlecenia tej płatności. |
| WSPŁ2 | Każda należność powinna zawierać co najmniej takie informacje jak: numer decyzji, naliczone odsetki oraz koszty upomnień i wezwań, czy był na nią wystawiony tytuł wykonawczy itp. |
| WSPŁ3 | Możliwość prezentowania i wyszukiwania konkretnej należności według rodzaju, daty, terminu płatności itp. |
| WSPŁ4 | Jeżeli należność została dopiero częściowo spłacona to użytkownik musi mieć możliwość otrzymania pełnej informacji w układzie: ile było wpłat na daną należność, kwota każdej płatności, data płatności oraz informację czy płatność została już zaksięgowana czy nie i saldo do zapłaty. |
| WSPŁ5 | Możliwość wyświetlania historii wszystkich interakcji finansowych mieszkańca z urzędami, jakie zostały zrealizowane poprzez systemy dziedzinowe zintegrowane. |
| WSPŁ6 | Aplikacja musi być zintegrowana z systemami bankowymi, w celu umożliwienia uregulowania należności online. |
| WSPŁ7 | Aplikacja musi pozwalać na wnoszenie opłat za pośrednictwem systemu płatności elektronicznych w różny sposób tzn. przez wygenerowanie płatności na wybraną należność i opłacenie, lub na zaznaczenie kilku należności i zapłacenie je jednym przelewem. |
| WSPŁ8 | Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów należności. |
| WSPŁ9 | Jeśli należność jest płatna w ratach (np. należności podatkowe, należności rozłożone przez urząd na raty) portal winien również przedstawiać klientowi informację, którą ratę kwota płatności stanowi. |
| WSPŁ10 | W sytuacji, kiedy kilku klientów jest solidarnie zobowiązanych do zapłaty należności klient zalogowany do portalu musi widzieć również minimum imię, nazwisko i adres pozostałych współzobowiązanych. W przypadku podmiotów gospodarczych będzie to nazwa firmy i jej siedziba. |
| WSPŁ11 | W przypadku, jeśli należność powstała w drodze decyzji administracyjnej danego urzędu numer decyzji ma być również widoczny dla klienta wraz z nazwą urzędu z którego została wydana. |
| WSPŁ12 | Możliwość ukrycia wyświetlania wybranych parametrów należności wyszukiwanych na ekranie użytkownika. |
| WSPŁ13 | Aplikacja powinna posiadać mechanizmy kontroli i bezpieczeństwa chroniące użytkowników przed kilkukrotnym wniesieniem płatności z tego samego tytułu. |
| WSPŁ14 | Portal musi generować komunikaty informujące i/lub ostrzeżenia wizualne dla użytkownika podczas próby ponownego zlecenia płatności dla należności, dla których płatność została zlecona za pośrednictwem portalu a transakcja jeszcze jest przetwarzana. |
| WSPŁ15 | Możliwość wydrukowania wypełnionego polecenia przelewu bankowego lub pocztowego, dla zaznaczonej jednej lub zaznaczonych wielu należności. |
| WSPŁ16 | Możliwość wyszukiwania i prezentowania należności według jej rodzaju np. „pokaż tylko opłaty za dzierżawę” itp. |
| WSPŁ17 | Możliwość wyszukiwania i prezentowania należności według statusu płatności tzn. np. pokaż tylko zaległe itp. |
| WSPŁ18 | Powinna być możliwość zaznaczenia, ile dni przed terminem płatności powinna być wysłana informacja przypominająca do użytkownika. |
| WSPŁ19 | Powinna być możliwość określenia rodzaju wysłanej informacji przypominającej – mail czy sms, lub obie formy. |
| WSPŁ20 | Wygenerowane płatności zlecone za pośrednictwem portalu, ale jeszcze nie zaksięgowane powinny zawierać informacje takie jak: nazwa gminy dla której płatność została wygenerowana, nr konta bankowego na które została przelana płatność, kwota i data zlecenia, status zlecenia oraz data wykonania. |
| WSPŁ21 | Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów. |
| WSPŁ22 | Informacje o wygenerowanych płatnościach muszą być przesyłane z portalu do modułów systemu dziedzinowego właściwego urzędu. Proces przesyłania danych będzie działał w trybie online. |
| WSPŁ23 | Możliwość wyszukiwania lub filtrowania należności według co najmniej: nazwy gminy, konta bankowego na które została przelana płatność, rodzaju należności, kwoty, typu płatności, stanu zlecenia, daty zlecenia, |
| WSPŁ24 | Możliwość przeglądu operacji księgowych już zrealizowanych tzn. opłaconych (wpłaty, zwroty, przeksięgowania) |
| WSPŁ25 | Przegląd operacji księgowych już zrealizowanych na należnościach (wpłaty, zwroty, przeksięgowania) z wyszczególnionym dla każdej operacji co najmniej: jej rodzaju, konta bankowego na którym została zaksięgowana operacja, identyfikator, rok, rata, kwota, vat, odsetki, kwota zapłacona faktycznie, data i godzina przelewu. |
| WSPŁ26 | Możliwość ustawienia sortowania wyświetlanych danych rosnąco lub malejąco względem dowolnego z wyświetlanych parametrów. |
| WSPŁ27 | Możliwość ukrycia wyświetlania wybranych parametrów operacji. |
| WSPŁ28 | Możliwość wyszukiwania lub filtrowania zrealizowanych i zaksięgowanych operacji według co najmniej: Nazwy gminy, kontrahenta SD, rodzaju należności, terminu płatności od – do. |
| WSPŁ29 | Możliwość grupowania klientów urzędu w bazie portalu według kryteriów przyjętych przez Stowarzyszenie Wielkie Jeziora Mazurskie 2020, niezależnie od pogrupowania tych klientów w dotychczasowych systemach dziedzinowych urzędów. |
| WSPŁ30 | Dla należności dotyczących nieruchomości system musi prezentować dodatkowo minimum: numer decyzji, typ nieruchomości, numer nieruchomości, numer dokumentu własności/władania, datę wydania dokumentu – pobrane z SD. |
| WSPŁ31 | Dla należności dotyczących wydanych koncesji na sprzedaż napojów alkoholowych system musi prezentować dodatkowo minimum: typ koncesji, numer koncesji, datę wydania, stan zezwolenia, dat ważności zezwolenia od – do. |
| WSPŁ32 | Dla należności dotyczących podatku od osób prawnych system musi prezentować dodatkowo rok wydania decyzji, typ dokumentu, rodzaj podatku. |
| WSPŁ33 | Dla danych upomnienia system musi prezentować dodatkowo: numer upomnienia, rok upomnienia, koszt upomnienia, datę wydania upomnienia, datę odbioru upomnienia, kwotę do zapłaty. |

## Zapewnienie bezpieczeństwa transmisji danych za pomocą dedykowanych łączy

Poniżej zdefiniowano wymagania wdrożeniowe dotyczące zarówno Projektu jak i Systemu.

Celem integracji jest automatyzacja wymiany informacji podatkowych oraz stanów spraw pomiędzy SUE a lokalnymi Szynami Danych. Integracja będzie realizowana za pomocą Centralnej Szyny Danych.

Tabela 29 Parametry minimalne centralnej szyny danych oraz minimalny zakres usług bezpieczeństwa transferu danych

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WD1 | System SUE zostanie zainstalowany na infrastrukturze Wykonawcy i udostępniony. |
| WD3 | System SUE zostanie udostępniony zarówno dla pracowników urzędów Stowarzyszenia Wielkie Jeziora Mazurskie 2020 jak i mieszkańców i przedsiębiorców tego terenu. |
| WD2 | Systemu musi być zintegrowany z platformą ePUAP zapewniając bezpieczną i zautomatyzowaną wymianę metadanych i danych pomiędzy, a e-formularzami umieszonym na ePUAP. |
| WD3 | Standardy interfejsów wymiany danych pomiędzy EZD PUW i SUE muszą być zgodne z obowiązującymi przepisami prawa:  - Zgodnie z Art. 16 ustawy z dnia ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005r. Nr 64, poz. 565, z późń. zm.)  - Interfejsy komunikacyjne wykorzystują komunikaty w formacie XML, opisane odpowiednimi schematami XMLSchema;  - Usługi sieciowe (WebService) udostępniane przez poszczególne systemy muszą być opisane zgodnie ze standardem języka opisu usług sieciowych WSDL (Web Services Description Language). Wszystkie wywołania usług WebService są wywoływane z wykorzystaniem szyfrowania SSL;  - Dane opisujące dokumenty przesyłane pomiędzy systemami podlegającymi integracji muszą spełniać wymogi dla dokumentów elektronicznych i być zgodne z przestrzenią nazw publikowaną w portalu ePUAP. |
| WD4 | System integracji SUE zapewni świadczenie usług elektronicznych na Poziomie 4 – Transakcja, wg klasyfikacji Poziomów usług elektronicznych. |
| WD5 | Wymiana informacji w sposób niezależny od użytych technologii musi zostać zrealizowana z  wykorzystaniem standardów Web Services. |
| WD6 | Funkcje integracji zostaną zrealizowane poprzez wykonanie, dostarczenie i wdrożenie przez Wykonawcę Oprogramowania interfejsowego. |
| WD7 | Zamawiający wymaga aby SUE dostępny był u każdego uczestnika projektu poprzez wydzielone łącze transmisji danych o przepustowości minimalnej 100 Mbps symetrycznej. |
| WD8 | Zamawiający wymaga aby wszyscy uczestnicy projektu uzyskali dostęp do SUE za pomocą sieci VPN z wykorzystaniem protokołu MPLS. Usługa musi posiadać strukturę płaską składającą się z routerów w lokalizacji centralnej Data Center w chmurze IAAS oraz routerów w lokalizacjach JST. Wszystkie routery wchodzące w skład usługi połączone zostaną w topologii Full MESH i będą komunikować się ze sobą poprzez sieć MPLS w technologii IP MPLS .  Zamawiający wymaga aby urządzenia te zostały tak dobrane by w przyszłości istniała możliwość zwiększenia wymaganych przepustowości łączy poszczególnych lokalizacji do min. 500 Mbps na JST.  Usługa dla urzędów powinna składać się z  I. Lokalizacji centralnej Data Center   * dołączonej do usługi dwoma łączami w technologii gigabit Ethernet na których zostaną skonfigurowane kanały z pasma 800 megabitów na sekundę. Data Center zostanie podłączony do sieci MPLS w strukturze 2CE-2PE zostaną tam zainstalowane dwa routery. * dołączonej do sieci Internet pasmem do 800 Mbps   II. Lokalizacjach terenowych   * zostaną podłączone do sieci MPLS w strukturze CE-2PE łączami podstawowymi zrealizowanych w technologii Ethernet z pasem min. 100 Mbps i  łączami zapasowymi zrealizowanymi w technologii 3G/LTE. W lokalizacjach tych zostaną zainstalowane routery z wymaganym wyposażeniem i kartami SIM pozwalającymi na zrealizowanie połączenia zapasowego w okresie trwałości projektu. |
| WD9 | Dostęp do Internetu w Data Center.  W Data Center zostanie zrealizowany dostęp do internetu, do którego dostęp konfiguracyjny będą posiadać uprawnienia pracownicy Lokalnego Centrum Kompetencji (JST). Połączenie będzie zrealizowane z wykorzystaniem kanału logicznego o przepustowości min. 800 Mbps. Kanał ten będzie realizował dostęp do Data Center dla użytkowników z Internetu. Zamawiający wymaga aby dostęp do internetu z Data Center dla urządzeń znajdujących się w urzędach został ograniczony w przypadku ruchu wychodzącego i przychodzącego do następujących usług:   * pop3 * SSL pop3 * IMAP * SSL imap * smtp * SSL smtp * http * https   Lista usług musi być możliwa do zmodyfikowania (zarówno dodana nowa jak i zablokowana) przez uprawnionego pracownika Lokalnego Centrum Kompetencji. Zamawiający wymaga także aby na tym łączu dostępna była min. 22 adresowa podsieć adresów publicznych.  Pracownik Lokalnego Centrum Kompetencji musi mieć możliwość dowolnego sposobu przydzielania adresów publicznych. |
| WD10 | Zamawiający wymaga aby w celu zapewnienia największej efektywności systemu na styku z segmentem publicznym, segment bezpieczeństwa zlokalizowany został za  routerami  realizującymi dostęp do sieci  MPLS  w Data Center operatora.  W celu zapewnienia ciągłości świadczonych usług zostanie musi być zastosowana redundancja na poziomie routerów i firewalla. |
| WD11 | Zarządzanie pasmem QoS.  Zamawiający wymaga wprowadzenia przez operatora Data Center i łącz dostępowych możliwości ustawiania priorytetów ruchu w celu zapewnienia lepszych parametrów jakościowych dla aplikacji krytycznych dla działania urzędów i bardziej efektywnego wykorzystania zakupionego pasma IP łączy podstawowych dostępnych będzie 5 klas usługowych dla transmisji danych oraz  dwie dedykowane do transmisji głosu i wideo.  Opis klas   * klasa V1 - klasa usługowa z zastosowanym mechanizm ml lq zapewniających bezwzględne pierwszeństwo pakietów z kolejki. * klasa V2- klasa Usługowa dedykowana do transmisji obrazu * klasa D1 - klasa Usługowa z najwyższym priorytetem dla ruchu do transmisji danych, w przypadku wystąpienia przeciążenia w sieci jest wykorzystywana przez aplikacje krytyczne dla działania Partnerów Projektu, wrażliwe na straty pakietów i opóźnienia, * klasa D2 klasa Usługowa ze średnim priorytetem dla transmisji danych reprezentująca zwykły poziom jakości usługi jest wykorzystywana dla aplikacji typu standardowego, * klasa D3 obejmująca ruch bez Gwarantowanych parametrów - najniższy priorytet wśród klas w ruchu dla transmisji danych przeznaczona jest dla pozostałych aplikacji klienta które nie są krytyczne dla działania Partnerów Projektu. |
| WD12 | Wymagania zamawiającego dotyczące sieci WAN/MPLS :  przepustowość usług:  - dla lokalizacji głównej oczekiwana przepustowość łącza do MPLS wynosi min. 800 Mb/s  - dla pozostałych lokalizacji oczekiwana przepustowość łączy wynosi min. 100 Mb/s   1. Zamawiający wymaga aby usługa miała charakter kompleksowy i obejmowała wszystkie wyżej wymienione lokalizację zamawiającego a także lokalizację główną czyli Data Center wykonawcy. 2. wykonawca będzie świadczył usługę transmisji danych w oparciu o sieć IP/MPLS wykonawcy na bazie łączy dostępowych zarządzanych przez Wykonawcę do routerów CE zainstalowanych w miejscach wskazanych przez zamawiającego. 3. W ramach świadczenia usługi wykonawca zainstaluje routery, przeprowadzi konfigurację oraz będzie odpowiadał za ich utrzymanie to jest zarządzanie usuwanie awarii według SLA wprowadzanie zmian konfiguracyjnych przez cały okres obowiązywania umowy 4. Wszystkie zestawione łącza podstawowe muszą być symetryczne 5. W wydzielonej sieci pakietowej wykonawcy powinna istnieć możliwość komunikacji na zasadzie każdy z każdym tak aby połączenia mogły być nawiązywane pomiędzy lokalizacjami zamawiającego przy założeniu uzyskania przepustowości połączenia równej najmniejszej przepustowości dostępowej w danej lokalizacji 6. Zamawiający wymaga zakończenia na urządzeniu dostępowym wykonawcy w postaci interfejsu Ethernet full-duplex lub kompatybilnego10/100/1000 Base-Tx. 7. Zamawiający wymaga aby w lokalizacji głównej łącza dostępowe zostały zestawione w konfiguracji 2CE-2PE  polegającej na instalacji dwóch routerów dostępowych CE które są połączone z dwoma różnymi routerami szkieletowymi wykonawcy PE za pomocą dwóch niezależnych rozłącznych tras. 8. Zamawiający wymaga aby łącza dostępowe w lokalizacji głównej podstawowe i zapasowe były zrealizowane za pomocą medium przewodowego. 9. zamawiający wymaga aby w lokalizacjach  poza lokalizacją główną łącza dostępowe zostały zestawione w  konfiguracji CE-2PE  polegającej na instalacji routera dostępowego CE  które są połączone z dwoma różnymi routerami szkieletowymi wykonawcy PE za pomocą dwóch  niezależnych i rozłącznych tras zamawiający wymaga aby jedno z dwóch łączy dostępowych było realizowane  za pomocą medium przewodowego (kabel światłowodowy)  Natomiast drugie łącze dopuszczone jest do realizacji jako łącze radiowe w technologii LTE, działające w oparciu o sieci komórkowe operatorów GSM. 10. ze względu na wymagania w zakresie bezpieczeństwa zamawiający wyklucza możliwość zbudowania łączy dostępowych z wykorzystaniem:  * łączy satelitarnych * łączy radiowych działających w paśmie niekoncesjonowanym * Łączy radiowych typu punkt wielopunkt * technologii IEEE801.11  1. Zamawiający wymaga aby wykonawca zapewnił w swojej sieci MPLS transmisję typu unicast oraz multicast. |
| WD13 | Bezpieczeństwo i ochrona przed atakami:  W ramach postępowania Wykonawca dostarczy Zamawiającemu min. usługi:   1. Ochrona przed atakami znanymi atakami na usługi i serwery (np. DoS, DDoS, Ping of Death, MITM, itp.), 2. Cloud Firewall (w tym min.: IDS, IPS, Antivirus, WebFilter, DomainReputation), 3. AntyMalware, 4. Web Application Firewall, 5. Secure Cloud Mail Gateway (z funkcją antyspam i antywirus),   W ramach umowy wykonawca uruchomi skonfiguruje oraz będzie utrzymywał wyżej wymienione usługi na rzecz zamawiającego przez okres trwania umowy.  Wykonawca zapewni pełne wsparcie techniczne ekspertów na wszystkich etapach współpracy, łącznie z okresem przedwdrożeniowym. Wsparcie to będzie obejmowało analizę faktycznych potrzeb Zamawiającego, analizę posiadanej infrastruktury oraz poprawne uruchomienie usług adresujących potrzeby Zamawiającego w obszarze cyber-bezpieczeństwa.  Wykonawca będzie świadczył aktywny monitoring usług bezpieczeństwa zasobów IT Zamawiającego i reagował na ataki z wykorzystaniem specjalizowanego zespołu Security Operations Center (SOC).  Zamawiający będzie miał dostęp do raportów on-line, natomiast niezależnie od tego Wykonawca musi oferować Zamawiającemu wsparcie (telefoniczne jak i mailowe) w trybie 24/7/365.  **I. Ochrona przed atakami**  Ochrona przed atakami, to usługa ochrony zasobów oraz aplikacji Zamawiającego zarówno przed atakami wolumetrycznymi jak i atakami aplikacyjnymi typu DoS.  W celu poprawnego świadczenia usługi Ochrony przed atakami Wykonawca musi posiadać zlokalizowany na terenie Polski system bezpieczeństwa zapewniający ochronę w warstwach ISO/OSI: od warstwy 3 do warstwy 7. Wymagany zakres funkcjonalny ochrony:   1. Wykonawca ma świadczyć usługę ochrony przed atakami typu DoS na łączu wykonanym w technologii światłowodowej; 2. Usługa musi być monitorowana w sposób ciągły (24/7/365), z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i w efekcie utratą ciągłości procesów biznesowych; 3. Monitoringiem i obsługą incydentów związanych z atakami musi zajmować się zespół Security Operations Center (SOC), realizujący wyłącznie funkcje nadzoru, działająca w trybie 24/7/365; 4. Wykonawca musi posiadać co najmniej dwie niezależnie działające linie wsparcia dedykowane do obsługi wyłącznie incydentów z obszaru bezpieczeństwa. Pierwsza linia wsparcia musi pełnić funkcje monitoringu i operacyjnej ochrony przed atakami oraz prowadzić ciągły dyżur przez co najmniej dwie osoby. Druga linia wsparcia będzie realizowała funkcję poszukiwania, analizowania i rozwiązywania niestandardowych problemów związanych z obsługa incydentów w zakresie bezpieczeństwa; 5. W ramach usługi konieczne jest zapewnienie całodobowej gotowości do podjęcia reakcji w czasie nie dłuższym niż 15 minut od momentu wykrycia ataku; 6. Jednostka wewnętrzna Wykonawcy realizująca obsługę incydentów związanych z atakami musi zapewniać na potrzeby Zamawiającego komunikację w języku polskim; 7. Monitorowanie ruchu powinno być przeprowadzane przy wykorzystaniu technologii bazujących na przepływach pakietów IP takich jak np. NetFlow czy sFlow; 8. Muszą być gromadzone informacje o wszystkich połączeniach do systemów usługowych Zamawiającego poprzez wykorzystanie protokołu typu NetFIow lub podobnych; 9. Przełączanie ruchu Zamawiającego w przypadku ataku powinno być realizowane za pomocą protokołu BGP; 10. Rozwiązanie powinno umożliwiać stosowanie szeregu technik w celu powstrzymywania (mitygacji) ataków DoS, co najmniej w zakresie:     1. Blokada niedozwolonych zapytań;     2. Blokada niedozwolonych zapytań DNS;     3. Blokada ataków typu TCP Floods (np: SYN, ACK+FIN, RST, SYN+ACK, Fragmentation), UDP floods, ICMP floods, IGMP floods;     4. Blokada niepożądanego ruchu w oparciu o unikalne, automatycznie generowane do każdego ataku sygnatury w oparciu między innymi o: adres(y) IP/źródłowy/docelowy, port(y) źródłowy/docelowy, rozmiar pakietu, TTL, checksum, sequence numer, ID, offset;     5. Wykrywanie i blokada pakietów nienależących do sesji (out of state);     6. Geolokalizacja adresów IP, umożliwiająca blokadę ruchu pochodzącego z danego kraju bądź regionu geograficznego;     7. Dopuszczanie, blokada, lub ograniczenie pasma (policing) dla ruchu pochodzącego z krajów z którymi w normalnych warunkach Zamawiający nie utrzymuje współpracy;     8. Limitowanie ilości połączeń jak i ilości pakietów na sekundę (dla połączenia lub globalnie) per dowolny port docelowy (aplikacja);     9. Listy przepuszczające ruch z krytycznych serwisów i lokacji, lub blokujące spoofowane adresy oraz ruch obserwowany na niewłaściwych portach;     10. Listy przepuszczające ruch pochodzący ze znanych i zaakceptowanych lokalizacji, oraz blokujące ruch pochodzący od zainfekowanych hostów i serwerów będących pod kontrolą botnetów;     11. Monitorowanie podsieci i protokołów w celu identyfikacji ruchu o parametrach wyższych niż zdefiniowane;     12. Ochrona serwerów Web poprzez przepuszczanie zapytań http zgodnych z RFC oraz pochodzących z właściwych źródeł;     13. Wykonywanie deszyfrowania/szyfrowania pozwalające na inspekcję danych wewnątrz tunelu SSL/TLS;     14. Inspekcja ruchu w celu identyfikacji ataków przeprowadzanych na podatności payload;     15. Ochrona przed ruchem IP powodującym przepełnienie tablicy stanu dla serwerów, urządzeń bezpieczeństwa typu firewall i urządzeń równoważących obciążenie;     16. Ochrona serwerów przed atakiem polegającym na podtrzymywaniu bezpodstawnie długiej sesji;     17. Ochrona serwerów DNS, realizowana co najmniej poprzez:         1. ochronę przed atakami typu floods na zapytania;         2. automatyczne budowanie stanu początkowego (tzw. „baseline”), ciągły proces modyfikacji wagowej wraz ze zmieniającymi się parametrami ruchu;         3. logikę wykrywania ataków opartą o parametry ilościowe (np. liczba zapytań na sekundę) i odchylenie od stanu początkowego (stosunek do siebie zapytań różnego typu, min.: A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV, pozostałe);         4. blokowanie niepożądanego ruchu w oparciu o unikalne, automatycznie generowane do każdego ataku sygnatury w oparciu między innymi o: adres(y) IP/źródłowy/docelowy, port(y) źródłowy/docelowy, rozmiar pakietu, TTL, DNS ID, DNS QNAME; możliwość wyboru ignorowanych parametrów w pakiecie: np. port źródłowy, ToS, VLAN tag;         5. autentykację klientów (dla zapytań A i AAAA) poprzez selektywne odrzucanie zapytań;     18. Ochrona przed atakami SYN Flood, realizowana co najmniej poprzez:         1. aktywację po przekroczeniu skonfigurowanego progu per dowolny port docelowy (aplikacja);         2. autentykację klientów z wykorzystaniem metod: transparent proxy (SYN cookie), Safe-Reset (ACK z niewłaściwym polem sequence number) oraz dla wspieranych protokołów TCPReset-Data i TCPReset-ACK, autentykacja z wykorzystaniem kodu HTTP 302 lub JavaScript dla protokołu http;     19. Inspekcję intruzów (Instrusion Prevention System), w tym blokowanie ataków na systemy operacyjne, serwery WEB, bazy danych i protokoły;     20. Behawioralne wykrywanie i blokowanie prób skanowania zasobów;     21. Behawioralna ochrona aplikacyjna protokołu http, realizowana co najmniej poprzez:         1. automatyczne budowanie stanu początkowego (tzw. „baseline”), ciągły proces modyfikacji wagowej wraz ze zmieniającymi się parametrami ruchu;         2. wykrywanie i blokowanie anomalii w stosunku do tzw. „baseline” w ilościach żądań GET i POST, w ilościach żądań innych niż GET i POST, ilości żądań per IP lub połączenie TCP, oraz w wykorzystywanym paśmie wychodzącym;         3. selektywna autentykacja klientów z wykorzystaniem kodu HTTP 302 lub JavaScript dla protokołu http;     22. Wykrywanie i blokowanie ataków typu Brute Force na serwisy Zamawiającego, w tym min.: HTTP, DNS, FTP, IMAP, LDAP, MS SQL, MySQL, POP3, SIP, SMTP;     23. Wykrywanie anomalii w pakietach, min. Invalid TCP Header Length, Invalid UDP Header Length, Invalid TCP Flags, Unsupported L4 Protocol, Invalid IPv4 Header or Total Length, Incorrect IPv4 Checksum, Unrecognized L2 Format, TTL Less Than or Equal to 1, Inconsistent IPv6 Headers, IPv6 Hop Limit Reached, Source or Destination Address same as Local Host, Source Address same as Dest. Address, L4 Source or Destination Port Zero;     24. Mechanizmy zarządzania pasmem; 11. Konieczne jest raportowanie do Zamawiającego o każdym wykrytym ataku na infrastrukturę Zamawiającego. 12. Wykonawca musi dostarczać okresowe (min raz na kwartał) raporty na temat monitorowanego ruchu oraz ilości i rodzajów ataków przeprowadzonych na infrastrukturę Zamawiającego.   **II. Cloud Firewall**  Cloud Firewall, to usługa zapewniająca ochronę dostępu do sieci Internet oraz zasobów IT Zamawiającego. Oferowana usługa, musi mieć możliwość utworzenia unikalnego profilu bezpieczeństwa, umożliwiający zastosowanie ściśle dopasowanych polityk bezpieczeństwa, dla każdej Jednostki Samorządu Terytorialnego (JST) biorącej udział w projekcie.  W celu poprawnego świadczenia usługi Cloud Firewall, Wykonawca musi posiadać na terenie Polski system bezpieczeństwa, zbudowany w architekturze HA zapewniający następujące funkcjonalności:   1. Zaporę sieciową (Firewall); 2. Kontrolę aplikacji (Application Control); 3. Inspekcję intruzów (Instrusion Prevention System); 4. Antywirus; 5. Bezpieczny zdalny dostęp do zasobów (IPSec/SSL VPN); 6. Inspekcję ruchu SSL; 7. Ochronę przed wirusami, co najmniej dla protokołów: SMTP, POP3, IMAP, HTTP, FTP, HTTPS; 8. Kontrolę stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM; 9. Kontrolę zawartości poczty - antyspam dla protokołów: SMTP, POP3, IMAP; 10. Kontrolę pasma oraz ruchu; 11. Ochronę przed wyciekiem danych (DLP). 12. Wymagane jest aby usługa w zakresie funkcji IPSec VPN, oferowała nie mniej niż: 13. Tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site; 14. Monitorowanie stanu tuneli VPN oraz stałe utrzymywania ich aktywności; 15. Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF; 16. Obsługę mechanizmów: IPSec NAT Traversal, DPD, XAuth; 17. Wymagania minimalne dotyczące wydajności usługi Cloud Firewall: 18. musi obsłużyć nie mniej niż 2 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę. 19. musi obsłużyć przepustowość Firewall na poziomie nie mniej niż 20 Gbps. 20. musi obsłużyć przepustowość nie mniej niż 9 Gbps podczas połączeń szyfrowanych VPN IPSec. 21. musi obsługiwać przepustowość minimum 6 Gbps podczas skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS). 22. wydajność skanowania typowego ruchu z włączonymi funkcjami IPS, AC, AV musi obsługiwać minimum 1 Gbps.   Polityka bezpieczeństwa usługi Cloud Firewall musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.  Silnik antywirusowy oferowany w ramach usługi, musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach oraz musi umożliwiać skanowanie archiwów spakowanych typu ZIP, RAR.  Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków musi zawierać minimum 5000 wpisów. Dodatkowo musi istnieć możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS oraz podobnymi.  Funkcja Kontroli Aplikacji, powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Baza filtra WWW oferowanej usługi powinna być wielkości co najmniej 40 milionów adresów URL, pogrupowanych w kategorie tematyczne. W ramach filtrowania stron internetowych, powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance.  Usługa musi zapewniać automatyczną aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.  W ramach usługi Wykonawca udostępni centralny system logowania i raportowania. System musi stanowić centralne repozytorium gromadzonych danych syslog, z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. System logowania i raportowania musi zapewniać:   1. Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników; 2. Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci; 3. Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących; 4. Wyświetlanie nowych logów w czasie rzeczywistym; 5. Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji z możliwością jej zapisu i późniejszej analizy; 6. Export zgromadzonych logów do zewnętrznych systemów składowania danych. 7. Możliwość robienia cyklicznych exportów logów do zewnętrznego systemu logowania w celu wydłużenia czasu składowania logów za pomocą następujących protokołów FTP, SFTP, SCP; 8. Musi oferować podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:    1. Listę najczęściej wykrywanych ataków;    2. Listę najbardziej aktywnych użytkowników;    3. Listę najczęściej wykorzystywanych aplikacji;    4. Listę najczęściej odwiedzanych stron WWW;    5. Listę krajów , do których realizowana jest komunikacja;    6. Listę najczęściej wykorzystywanych polityk Firewall;    7. Informacje o realizowanych połączeniach IPSec; 9. W zakresie raportowania system musi zapewniać:    1. Generowanie raportów co najmniej w formatach: HTML, PDF, XML, CSV;    2. Predefiniowane zestawy raportów;    3. Funkcję definiowania własnych raportów;    4. Generowanie raportów cyklicznie lub na żądanie, za możliwością automatycznego przesłania wyników na określony adres lub adresy email; 10. W zakresie korelacji zdarzeń system musi korelować zdarzenia co najmniej dla następujących kategorii eventów:     1. Malware;     2. Kontroli aplikacji;     3. Email;     4. IPS;     5. Traffic;     6. Systemowe, min. utracone połączenie VPN i/lub utracone połączenie sieciowe; 11. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów.   **III. Antymalware**  Antymalware, czyli usługa umożliwiająca wykrycie złośliwego oprogramowania, Advanced Persistent Threat (APT), a także zagrożeń typu „zero-day”.  W celu poprawnego świadczenia usługi Antymalware, Wykonawca musi posiadać na terenie Polski bezpieczne, wyizolowane, wirtualne środowisko testowe (Sandbox) pozwalające na:   1. Analizę internetowego ruchu przesyłanego pomiędzy zasobami IT Zamawiającego a siecią Internet, na łączu, na którym uruchomiono usługę; 2. Skanowanie zawartości przesyłanej z zastosowaniem protokołów http, https, imap, pop3, smtp i ftp; 3. Rozpoznawanie plików i kwalifikację ich na: bezpieczne, złośliwe oraz podejrzane, przy czym po analizie:    1. pliki bezpieczne są przepuszczane dalej;    2. pliki znane, szkodliwe są automatycznie blokowane;    3. pliki pojawiające się o nieznanej charakterystyce, podejrzane, są testowane w środowisku wirtualnym i sprawdzane. 4. Testowanie podejrzanego pliku:    1. jeżeli plik nie jest zagrożeniem, jego sygnatura jest dodawana do bazy plików z informacją, że plik nie wymaga dodatkowej analizy i jest bezpieczny;    2. jeżeli plik posiada zagrożenie, jego sygnatura jest dodawana do bazy plików z informacją, aby plik był blokowany przez platformę Sandbox. 5. Wykrywane i blokowanie komunikacji z infrastrukturą Command and Control (C&C) nadzorowaną przez cyber-przestępców, w przypadku, kiedy dojdzie do infekcji stacji roboczej (np. poprzez email, pendrive, gmail, https lub pierwsze przesłanie nieznanego malware’u); 6. Dostarczanie informacji do administratorów IT/bezpieczeństwa Zamawiającego o wykrytych zagrożeniach lub podejrzeniach ataków, celem podjęcia innych niezbędnych działań (np. usunięcia malware ze stacji użytkownika czy innych działań zapobiegawczych). Informacje te będą udostępnione w formie logów i statystyk poprzez autoryzowaną stronę WWW oraz za pośrednictwem poczty elektronicznej. Zamawiający poprzez autoryzowaną stronę WWW, ma mieć dostęp do graficznej prezentacji zebranych danych w funkcji czasu, w postaci wykresów tygodniowych, miesięcznych, rocznych jak i z dowolnie wybranego okresu.   **IV. Web Application Firewall**  Web Application Firewall (WAF), czyli usługa ochrony serwisów web’owych (WWW) Zamawiającego przed zagrożeniami z sieci Internet skierowanymi na aplikacje WEB .  Usługa chroni zasoby Zamawiającego analizując żądania wysyłane z Internetu do serwerów WWW i akceptując tylko te, które:   * spełniają kryteria poprawności protokołu komunikacyjnego (zgodność ze standardami/RFC); * są zgodne ze skonfigurowaną polityką bezpieczeństwa.   Usługa ma poddawać inspekcji zarówno zawartość serwisu, jak i protokoły służące do jego dostarczenia, np. HTTP, HTTPS.  W celu poprawnego świadczenia usługi Web Application Firewall, Wykonawca musi posiadać na terenie Polski system bezpieczeństwa zbudowany w architekturze HA posiadający co najmniej następujące funkcjonalności:   1. Inspekcja warstwy 7; 2. Możliwość definiowania nazw parametrów i oczekiwanych wartości parametrów; 3. Wykrywanie i blokowania ataków typu „brute force” na hasła użytkowników; 4. Wsparcie dla XML:    1. Walidacja schematu/WSDL;    2. Wybór dozwolonych metod SOAP;    3. Sygnatury ataków XML; 5. Możliwość definiowania polityk per URI aplikacji; 6. Wsparcie dla technologii Asynchronous JavaScript + XML i JavaScript Object Notation; 7. Możliwość zabezpieczenia aplikacji przed atakami DoS na poziomie URI; 8. Możliwość blokowania użytkowników per kraj, z którego przychodzi ruch lub pochodzi atak (IP Geolocation); 9. Możliwość integracji ze skanerami podatności aplikacji firm trzecich w celu budowania polityk; 10. Filtrowanie odpowiedzi serwera jak i kodów błędu; 11. Możliwość ukrycia zasobów serwera; 12. Musi posiadać mechanizmy monitorowania stanu serwerów; 13. Musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone) jak i negatywny model bezpieczeństwa (funkcje identyfikacji incydentów poprzez sygnatury); 14. Musi posiadać możliwość automatycznego tworzenia modelu bezpieczeństwa na podstawie ruchu do aplikacji Web; 15. Musi istnieć możliwość ograniczania zaufanych adresów źródłowych, z których komunikacja z aplikacją tworzyć będzie oczekiwany profil zachowań użytkowników; 16. Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr; 17. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki dostępu; 18. Musi posiadać mechanizmy ochrony przed atakami: SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Session hijacking, Command Injection, Cookie/Session Poisoning, Parameter/Form Tampering, Forceful Browsing, Brute Force Login; 19. Musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http); 20. Musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku DoS np. poprzez wstrzykiwanie skryptu w przypadku wystąpienia podejrzenia ataku; 21. Musi istnieć możliwość doboru odpowiedzi w zależności od rodzaju naruszenia; 22. Musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o kliencie oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez jednego klienta; 23. Musi realizować ochronę protokołu http; 24. Musi szyfrować cookies; 25. Musi realizować multipleksacje zapytań http; 26. Musi istnieć możliwość translacji aplikacji webowej w standardzie HTTP 1.1 na standard HTTP 2.0 bez zmian w samej aplikacji (HTTP 2.0 gateway); 27. Musi realizować optymalizację i akceleracja aplikacji, w tym co najmniej:     1. Optymalizację protokołu TCP z predefiniowanymi profilami LAN i WAN;     2. TCP proxy z mechanizmem zamykania okna w stronę serwera WWW w przypadku zbyt wolnego odbierania danych przez klienta;     3. Wbudowany cache w celu trwałego przetrzymywania obiektów zdefiniowanych na podstawie URI;     4. Ignorowanie nagłówków w przeglądarce klienta dotyczących cache’owania (cache-control),     5. Multipleksację wielu zapytań http w tej samej sesji TCP;     6. Kompresję zwracanej zawartości http; 28. Musi posiadać wbudowany język skryptowy, bazujący na języku programowania Tool Command Language (TCL) lub równoważnym, z własnymi komendami; 29. Musi wspierać następujące tryby pracy:     1. Tryb wykrywania, logowania i blokowania ataków;     2. Tryb wykrywania i logowania ataków bez blokowania;     3. Tryb uczenia się bez blokowania;     4. Tryb bez wykrywania i blokowania ataków.   **V. Secure Cloud Mail Gateway**  Secure Cloud Mail Gateway, to usługa zapewniające ochronę poczty elektronicznej Zamawiającego zapewniająca kompleksową ochronę poczty antyspamową, antywirusową oraz antyspyware’ową.  W celu poprawnego świadczenia usługi Secure Cloud mail Gateway, Wykonawca musi posiadać na terenie Polski system bezpieczeństwa zbudowany w architekturze HA zawierający następujące funkcjonalności:   1. Usługa musi obsługiwać wszystkie domeny pocztowe Zamawiającego – bez limitu ilości; 2. Usługa musi obsługiwać nieograniczoną ilość skrzynek pocztowych Zamawiającego; 3. Tworzenie polityk filtrowania w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all); 4. Obsługa routingu poczty oraz zarządzanie kolejkami bazujące na politykach; 5. Ochrona poczty przychodzącej oraz wychodzącej; 6. Granularne, wielowarstwowe polityki wykrywania spamu oraz wirusów; 7. Skanowanie Antywirusowe oraz Antyspamowe definiowane na użytkownika w oparciu o atrybuty LDAP; 8. Routing poczty (email routing) w oparciu o LDAP; 9. Kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika); 10. Dostęp do kwarantanny poprzez WebMail lub POP3; 11. Archiwizacja poczty przychodzącej i wychodzącej, backup poczty do różnych miejsc przeznaczenia; 12. Whitelist’y definiowane dla użytkownika;   Usługa w zakresie ochrony antywirusowej oraz antyspyware’owej, musi realizować:   1. Skanowanie antywirusowe wiadomości SMTP; 2. Kwarantannę dla zainfekowanych plików; 3. Skanowanie załączników skompresowanych; 4. Definiowanie komunikatów powiadomień w języku polskim; 5. Blokowanie załączników ze względu na typ pliku; 6. Możliwość zdefiniowania co najmniej 200 profili antywirusowych;   Usługa w zakresie ochrony antyspamowej musi zapewniać poniższe metody filtrowania:   1. Heurystyczną analizę spamu; 2. Filtrowanie treści załączników; 3. Szczegółową kontrolę nagłówka wiadomości; 4. Filtrowanie w oparciu o filtry Bayes’a, z możliwością dostrajania dla poszczególnych użytkowników; 5. Filtrowanie poczty w oparciu o sumy kontrolne spamu; 6. Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF; 7. Analizę poczty w oparciu o dynamiczną bazę spamu; 8. Współpracę z zewnętrznymi serwerami RBL; 9. Kontrolę w oparciu o Greylist’y; 10. Białe i czarne listy definiowane globalnie oraz per użytkownik; 11. Kwarantannę oraz oznaczanie spamu; 12. Weryfikację źródłowego adresu IP; 13. Możliwość zdefiniowania co najmniej 200 profili antyspamowych;   Usługa musi posiadać ochronę przed następującymi atakami:   1. Denial of Service (Mail Bombing); 2. Ochrona przed atakami na adres odbiorcy; 3. Definiowanie maksymalnych ilości wiadomości pocztowych; 4. Kontrola Reverse DNS (Anty-Spoofing); 5. Weryfikacja poprawności adresu e-mail nadawcy;   W ramach usługi Wykonawca udostępni system logowania i raportowania. System logowania i raportowania udostępniony w ramach usługi musi zapewniać:   1. Powiadamianie o działalności wirusów; 2. Logowanie informacji na temat spamu oraz niedozwolonych załączników; 3. Predefiniowane szablony raportów; 4. Możliwość planowania czasu generowania raportów; 5. Możliwość podglądu logów w czasie rzeczywistym.     **VI. System ochrony serwerów w JST**  Usługa zabezpieczenia lokalnych serwerów, zainstalowanych w Jednostkach Samorządu Terytorialnego (JST) biorącej udział w projekcie.  W ramach dostarczonego systemu ochrony serwerów w JST muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:   1. Zaporę sieciową (Firewall); 2. Kontrolę aplikacji (Application Control); 3. Inspekcję intruzów (Instrusion Prevention System); 4. Bezpieczny zdalny dostęp do zasobów (IPSec/SSL VPN); 5. Inspekcję ruchu SSL; 6. Ochronę przed wirusami, co najmniej dla protokołów: SMTP, POP3, IMAP, HTTP, HTTPS, FTP; 7. Kontrolę pasma oraz ruchu;   Usługa System ochrony serwerów w JST musi obsługiwać nie mniej niż 1 mln. jednoczesnych połączeń oraz 85 tys. nowych połączeń na sekundę.  Usługa System ochrony serwerów w JST musi obsługiwać przepustowość Firewall na poziomie nie mniej niż 9 Gbps.  Wydajność szyfrowania VPN IPSec musi obsługiwać nie mniej niż 850 Mbps.  Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) musi obsługiwać minimum 3000 Mbps.  Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, AC, AV musi obsługiwać minimum 1500 Mbps.  Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) ) oraz powinien umożliwiać skanowanie archiwów typu zip, rar.  Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.  System logowania i raportowania udostępniony w usłudze Cloud Firewall musi być przystosowany do współpracy z usługą Ochrony serwerów w JST. Udostępniony System logowania i raportowania musi umożliwiać kolekcjonowanie logów z co najmniej 200 urządzeń.  **VII. Skanowanie bezpieczeństwa sieci i aplikacji webowych**  Usługa skanowania bezpieczeństwa sieci i aplikacji webowych, polega na zbadaniu, czy serwis Zamawiającego posiada błędy mogące narazić go na skompromitowanie. Zamawiający wymaga od Wykonawcy, aby w ramach usługi wykonywał cykliczny, minimum raz na kwartał, skan uzgodnionych zakresów IP.  Wykonawca do skanowania bezpieczeństwa sieci i aplikacji webowych musi wykorzystać komercyjny skaner podatności wraz z zestawem odpowiednio dobranych pluginów oraz innych narzędzi do skanowania sieci.  W ramach usługi, wykonawca musi przeprowadzić test infrastruktury Zamawiającego, której celem będzie identyfikacja podatności usług sieciowych dostępnych w testowanych systemach. Zadanie to musi być realizowane za pomocą testów automatycznych i następujących po nich weryfikacji manualnej przez testerów.  Zakres testów infrastruktury musi obejmować:   1. Identyfikację usług i portów widocznych na wskazanym zakresie adresów IP; 2. Aktualność wersji oraz konfigurację systemu operacyjnego i udostępnianych usług sieciowych; 3. Wykorzystywanie zbędnych usług sieciowych i zbędnych funkcjonalności w pozostałych usługach; 4. Odporność na znane podatności; 5. Używanie domyślnych lub słabych haseł; 6. Możliwość pozyskania szerszych informacji na temat infrastruktury testowanego systemu;   W ramach usługi, wykonawca musi przeprowadzić testy aplikacji webowych, bazujących na standardzie testowania aplikacji sieci WEB zawartym w „OWASP Testing Guide”. Testy aplikacji webowych mogą zostać przeprowadzone według metodologii „black box” lub „gray box”.  Zakres testów aplikacji webowych musi obejmować:   1. Uwierzytelnianie:    1. Polityka zarządzania kontami i hasłami;    2. Zmiana/reset hasła;    3. Domyślne konta;    4. Blokada konta z powodu nieudanych prób logowania;    5. Występowanie nieograniczonych prób logowania;    6. Zapamiętywanie loginu/hasła w przeglądarce;    7. poziom szczegółowości informacji o nieudanej próbie logowania; 2. Autoryzacja:    1. Przekroczenie uprawnień;    2. Nieautoryzowany dostęp do zasobów;    3. Dodatkowa autoryzacja/uwierzytelnienia dla kluczowych operacji;    4. Cross-Site Request Forgery (CSRF);    5. CAPTCHA; 3. Zarządzanie sesją:    1. Złożoność i przewidywalność identyfikatorów sesji;    2. Automatyczne wygaśnięcie sesji;    3. Wygaśnięcie sesji po wylogowaniu;    4. Akceptacja nieprawidłowych identyfikatorów sesji;    5. Dostęp do stron internetowych bez identyfikatora sesji;    6. Jednoczesne sesje dla tego samego konta;    7. Obecność poufnych informacji w parametrach sesji;    8. Modyfikacja parametrów sesji; 4. Sprawdzanie poprawności danych wejściowych:    1. Cross-Site Scripting;    2. SQL Injection;    3. reakcja aplikacji na nietypowe wartości parametrów ; 5. Kryptografia:    1. Szyfrowania kanału komunikacyjnego;    2. Wersja SSL;    3. Renegocjacja SSL;    4. Algorytmy szyfrowania obsługiwane przez serwer;    5. Długość kluczy kryptograficznych;    6. Ważność certyfikatu SSL;    7. Szyfrowanie poufnych danych wysłanych przez niezaszyfrowanym kanał; 6. logika biznesowa:    1. Weryfikacja limitów (np. długość parametrów/wartości);    2. Zaburzenia sekwencji operacji; 7. HTTP i serwer WEB;    1. Dane wrażliwe wysłane metodą GET;    2. Aktywne niestandardowe metody;    3. Możliwość listowania zawartości katalogów;    4. Możliwość sprawdzania zasobów serwera;    5. Obecność zbędnych zasobów na serwerze; 8. Inne:    1. Generowanie dużego obciążenia serwera;    2. Zapamiętywanie wrażliwych danych w formularzach;    3. Parametry cookies;    4. Dostęp do interfejsów administracyjnych;    5. Wrażliwe dane przechowywane po stronie klienta (kod HTML, pliki Flash, itp);    6. Analiza kodu zdekompliowanych plików Flash, apletów Java, plików Silverlight;    7. Możliwość wgrywania plików;    8. Clickjacking.   Zamawiający wymaga w ramach usługi, wymaga po każdym skanowaniu bezpieczeństwa sieci i aplikacji webowych, opracował raport podsumowującego przeprowadzone prace. Raport musi zostać opatrzony komentarzem ekspertów bezpieczeństwa i zawierać następujące elementy:   1. Listę wykrytych podatności; 2. Klasyfikację podatności (high, medium, low, info); 3. Referencje do opisów wykrytych podatności (lista CVE); 4. Wpływ ewentualnego wykorzystania podatności na bezpieczeństwo systemu; 5. Rekomendacje w zakresie wprowadzenia zalecanych zmian.   **VIII. Backup i archiwizacja danych**  Wymagana jest archiwizacja kopii zapasowych na nośniki taśmowe. Pod pojęciem archiwizacji rozumie się backup z długim czasem retencji.  Nośniki taśmowe muszą być przechowywane w innym miejscu niż realizowane są kopie zapasowe. Wymaga się archiwizowania wszystkich kopii miesięcznych na taśmach umożliwiających przechowywania danych przez czas trwałości projektu (5 lat od podpisania protokołu końcowego). Zamawiający wymaga aby taśmy raz w miesiącu przesyłane były do Zamawiającego. Koszt przesyłki lub transportu spoczywa po stronie Zamawiającego. Taśmy przesyłane będą za potwierdzeniem odbioru. Zamawiający wymaga aby wszelkie backupy wykonywane były dla każdej jednostki Zamawiającego oddzielnie (oddzielne pliki lub foldery dla każdego JST). Backup danych odbywać się będzie zgodnie z Polityką Backupu i Archiwizacji.  **IX. Szkolenia e-lerningowe Security Awareness**  Szkolenie e-lerningowe Security Awareness, ma być skierowane dla 500 pracowników podmiotów biorących udział w projekcie, którzy korzystają z komputerów oraz innych urządzeń teleinformatycznych;  Program szkolenia musi obejmować, następujące zagadnienia:   1. Podstawy bezpieczeństwa systemów informatycznych; 2. Phishing i różne odmiany ataków socjotechnicznych; 3. Włamania, złośliwe programy i inne zagrożenia w sieci i Internecie; 4. Portale społecznościowe i niebezpieczne usługi; 5. Zagrożenia aplikacji P2P, Chat i programów portable; 6. Podstawowe zasady ochrony komputerów PC; 7. Bezpieczne surfowanie WWW; 8. Bezpieczne użytkowanie Email; 9. Hasła i kody dostępu; 10. Konsekwencje lekceważenia zasad bezpieczeństwa;   Wymagania w zakresie szkolenia:   1. Szkolenie musi być opracowane w języku polskim; 2. Ścieżka audio szkolenia e-lerningowego musi być nagrana przez zawodowego lektora; 3. Materiał musi być podzielony na krótkie 5-10 minutowe lekcje; 4. Szkolenie musi być interaktywne i zawierać animacje, ćwiczenia praktyczne, quizy oraz pytania kontrolne sprawdzające przyswojoną przez uczestników wiedzę; 5. Pracownicy biorący udział w szkoleniu muszą mieć możliwość odbywania lekcji z dowolnego miejsca, w dowolnym czasie; 6. Pracownicy biorący udział w szkoleniu muszą mieć możliwość decydowania o tempie projekcji szkolenia, jak również mają mieć możliwość przerwania i powrócenia do kursu w dowolnym momencie oraz dostępu do wcześniej prezentowanych materiałów dydaktycznych;   Podmioty biorące udział w projekcie muszą posiadać aktualne informacje na temat stanu i postępów kształcenia wszystkich swoich pracowników.  **X. Pozostałe wymagania względem Wykonawcy:**  Wykonawca musi wykonać szczegółową dokumentację zawierającą opis zaproponowanych usług Security wraz z opisem konfiguracji oraz instrukcji dla przedstawicieli Zamawiającego odnośnie obsługi portalu na którym będą dostępne raporty.  Wykonawca przeszkoli przedstawicieli Zamawiającego z obsługi portalu, na którym będą dostępne raporty oraz z obsługi systemów bezpieczeństwa.  W okresie świadczenia usług adresujących potrzeby Zamawiającego w obszarze cyber-bezpieczeństwa, Wykonawca zapewni Zamawiającemu możliwość konsultacji w języku polskim z inżynierami o specjalizacji bezpieczeństwo w wymiarze 20 godzin miesięcznie, przy czym godziny niewykorzystane w danym miesiącu sumują się z godzinami przeznaczonymi do wykorzystania w miesiącu następnym.  Zamawiający będzie zgłaszał nieprawidłowe działanie usług adresujących potrzeby Zamawiającego w obszarze cyber-bezpieczeństwa telefonicznie i niezwłocznie potwierdzał faksem lub mailem. Przy czym za moment zgłoszenia uważa się dzień i czas wysłania faksu lub maila. Brak potwierdzenia przyjęcia przez Wykonawcę (faksem lub mailem) nie będzie uważany za brak zgłoszenia.  Dla pełnej rozliczalności logów wymagane jest aby Wykonawca uruchomił serwer NTP i skonfigurował wszystkie urządzenia we wszystkich 12 lokalizacjach do synchronizacji czasu z tym serwerem. Serwer ten powinien być zlokalizowany w lokalizacji centralnej oraz w każdej lokalizacji terenowej lokalny serwer NTP [zrealizowany jako maszyna wirtualna].  **Zaoferowane parametry wymienione w powyższej tabeli Wykonawca musi utrzymać na poziomie nie niższym przez okres 60 miesięcy wsparcia od momentu podpisania protokołu odbioru końcowego.** |

## Integracja SUE z Lokalnymi Szynami Danych

W celu dostarczenia zaawansowanych usług elektronicznych dla mieszkańców i przedsiębiorców urzędów Stowarzyszenia Wielkie Jeziora Mazurskie 2020 konieczne jest dostarczenie integracji do pakietu modułów SUE.

Integracja ta ma na celu dostarczenie informacji w sposób skutecznych i jednoznaczny z lokalnych Szyn Danych umiejscowionych u partnerów projektu do jednego centralnego SUE oraz niezbędnych danych z SUE do lokalnych systemów dziedzinowych i obiegów dokumentów poprzez Lokalne Szyny Danych w celu dokonania poprawnego rozliczenia i zaksięgowania. W każdym przypadku kiedy zachodzi potrzeba doprecyzowania sposobu czy zakresu przesyłanych danych Wykonawca zwróci się na piśmie do Zamawiającego, a ten w terminie 3 dni roboczych udzieli szczegółowych informacji pozwalających na prawidłową realizację transferu danych. Minimalny zakres danych niezbędnych do przesyłania zostanie ustalony po podpisaniu umowy ze względu na różnorodność możliwych do przesyłania danych przez różne systemy i  będzie zależał od możliwości transferowych dostarczanych elementów Systemu. Na etapie wdrożenia należy ustalić protokoły i porty komunikacji.

Tabela 30 Minimalny zakres integracji SUE z SB

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WISS1 | SUE musi udostępniać informację o płatnościach, które zrealizował dla odpowiedniej lokalnej szyny danych. |
| WISS2 | SUE musi umożliwiać skonfigurowanie dowolnej liczby zintegrowanych Lokalnych Szyn Danych. |
| WISS3 | SUE musi umożliwiać pobranie wszystkich danych udostępnianych przez Lokalne Szyny Danych z oznaczeniem, z którego źródła przyszła. |

## Wdrożenie

Wdrożenie ma na celu przeprowadzenie procesu umożliwiającego Zamawiającemu korzystanie z zakupionego systemu.

Wykonawca musi działać w oparciu o system zarządzania jakością zgodny z wymaganiami ISO 9001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny oraz w oparciu o system zarządzania jakością zgodny z wymaganiami ISO/IEC 27001 wydany przez jednostkę akredytowaną w zakresie projektowania, wdrażania i utrzymywania oprogramowania wspomagającego pracę jednostek administracji publicznej lub równoważny.

Tabela 31 Minimalny zakres prac wdrożeniowych

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WW1 | Wykonawca ma obowiązek przeprowadzenia analizy przedwdrożeniowej obejmującej:  - analizę dotychczasowego sposobu organizacji pracy w obszarach SUE  - analiza bezpieczeństwa transmisji danych pomiędzy systemami Lokalnych Szyn Danych z SUE. |
| WW2 | Wykonawca ma obowiązek uzgodnienia z Zamawiającym Planu wdrożenia obejmującego:  - listę wymaganych czynności wykonywanych po stronie Zamawiającego  - uzgodnienie sposobu odbioru procesu wdrożenia SUE~~.~~ |
| WW3 | W ramach usług wdrożeniowych, Wykonawca zrealizuje:   * Udostępnienie na infrastrukturze sprzętowej Zamawiającego systemu SUE na potrzeby procesu wdrożenia i szkolenia * Skonfiguruje warstwę sprzętową, systemową i sieciową gwarantując odpowiedni poziom bezpieczeństwa * Uzgodni i wdroży poziom bezpieczeństwa w obszarze integracji z systemami urzędów Stowarzyszenia Wielkie Jeziora Mazurskie 2020 * Będzie dokonywał aktualizacji systemu SUE oraz konfiguracji na potrzeby realizacji projektu. |

# Zakres 5. Przygotowanie i przeprowadzenie pakietów szkoleń.

Szkolenia mają na celu osiągniecie odpowiedniej wiedzy z zakresu używania systemu na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia, a w szczególności z procedurą migracji danych.

Tabela 32 Minimalny zakres szkoleń dla Administratorów

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WSZ1 | Szczegółowy zakres poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiający w ramach akceptacji harmonogramu i materiałów szkoleniowych. |
| WSZ2 | Wykonawca na etapie uzgadniania materiałów szkoleniowych przekaże minimalne wymagania, jakie powinni spełniać oddelegowani przez Zamawiającego, uczestnicy szkolenia. |
| WSZ 3 | Do każdego modułu wspomagającego obsługę obszarów działalności urzędu, Zamawiający wskaże osoby, które Wykonawca przeszkoli. |
| WSZ4 | Szkolenia będą realizowane w pomieszczeniach i na sprzęcie udostępnionym przez urząd. |
| WSZ5 | Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych. |
| WSZ6 | Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 15 użytkowników oraz szkoleń indywidualnych przy stanowiskowych dla grup jedno-, dwu- lub trzyosobowych. |
| WSZ7 | Wykonawca przeszkoli osoby pełniące obowiązki administratorów wskazanych przez Zamawiający w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych. |
| WSZ8 | Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu bazodanowego. Szkolenie musi obejmować co najmniej instalację, konfigurację bazy danych, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii. |
| WSZ9 | Uzgodnieniu pomiędzy stornami podlegają:  - Minimalne wymagania dla uczestników szkoleń,  - Harmonogram szkoleń grupowych i indywidualnych,  - Materiały szkoleniowe dla szkoleń grupowych,  - Listy obecności ze szkoleń grupowych i indywidualnych,  - Protokoły Odbioru Zadania dot. Szkoleń. |
| WSZ10 | Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować użytkownikom systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać pracownikom na rozpoczęcie pracy w systemie. |
| WSZ11 | Zamawiający oczekuje przeprowadzenia szkoleń grupowych nie więcej niż:  - 10 dni szkoleń z zakresu integracji w warstwie Lokalnej Szyny Danych |
| WSZ12 | Zamawiający oczekuje przeprowadzenia szkoleń grupowych w wymiarze:  - min. 5 dni szklenia z zakresu SUE, jednak nie większym niż 10 dni.  - min. 2 dni szkolenia dla Administratorów z zakresu SUE, jednak nie większym niż 5 dni. |

# Zakres 6. Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej.

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji projektu.

Tabela 33 Parametry minimalne dla dostarczonej dokumentacji

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WDP1 | Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego systemu oraz w ramach usług integracyjnych dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją Systemu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu. |
| WDP2 | Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego systemu oraz w ramach usług integracyjnych dokumentację Użytkownika – opis działania Systemu w zakresie niezbędnym do jego prawidłowego użytkowania. |
| WDP3 | Zamawiający wymaga, alby Wykonawca dostarczył do dokumentację Integracji systemów SUE i EZD. |
| WDP4 | Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów. |
| WDP5 | Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył instrukcję dostępu do systemów i sieci Internet zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów. |
| WDP6 | Dokumentacja musi być sporządzona w języku polskim. |

# Zakres 7. Świadczenie usługi serwisu

Świadczenie usługi serwisu ma na celu zapewnienie ciągłości sprawnego działania Systemu poprzez realizację działań naprawczych wynikających z analizy ujawnionych problemów, wykrytych Dysfunkcji systemów, niewłaściwego działania systemu, spadku wydajności, wykryciu zagrożenia włamania, itp. Zakres i warunki opisane w Załączniku nr 6 do Umowy.

Tabela 34 Minimalny zakres prac świadczonych w ramach usługi wsparcia i serwisu

|  |  |
| --- | --- |
| Nr. | Wymaganie |
| WG1 | Wykonawca zobowiązuje się do dostarczania wolnych od wad kolejnych wersji Systemu. |
| WG2 | Wykonawca zobowiązuje się do aktualizacji dokumentacji Użytkownika i/lub Administratora. |
| WG3 | Wykonawca zobowiązuję się do świadczenia konsultacji dla Administratorów w zakresie niezbędnych zmian w konfiguracji systemu. |
| WG4 | Wykonawca zapewni usługę wsparcia użytkowników udostępniając:   * Usługę typu helpdesk, udostępnioną pod adresem e-mail, numerem telefonu i numerem faksu * portal typu helpdesk – dostępny on-line w trybie 356/7/24, gdzie będą publikowane statusy zgłoszeń * przez niniejszy portal będą mogły być dokonywane zgłoszenia Dysfunkcji |
| WG5 | Wsparcie użytkowników obejmuje świadczenie usługi wsparcia technicznego, merytorycznego oraz konsultacji w celu utrzymania poprawnej pracy systemu zgodnego z wymaganiami zamówienia. W ramach usługi Wykonawca zobowiązany jest do udzielania odpowiedzi na pytania Użytkowników i Administratorów związane z bieżącą eksploatacją Systemu. |
| WG6 | Wykonawca zapewni w godzinach pracy Zamawiającego w dni robocze obecność specjalistów mających niezbędną wiedzę i doświadczenie z zakresu eksploatacji Systemów. |
| WG7 | Wykonawca zapewni wystarczającą ilość konsultantów do zapewnienia ciągłości usługi gwarancji. |
| WG8 | Wykonawca będzie świadczył na rzecz Zamawiającego usługi serwisu w zakresie przedmiotu zamówienia (umowy) w okresie 60 miesięcy (licząc od daty podpisania protokołu odbioru końcowego) zapewniając jednocześnie odpowiednie wsparcie merytoryczne. |
| WG9 | W ramach usługi Wykonawca zobowiązany jest do nieodpłatnego usuwania dysfunkcji:   * z przyczyn zawinionych przez Wykonawcę będących konsekwencją wystąpienia: Dysfunkcji w Systemie, błędu lub wady fizycznej pakietu aktualizacyjnego lub instalacyjnego, błędu w dokumentacji administratora lub w dokumentacji użytkownika, błędu w wykonaniu usług przez Wykonawcę; * związanych z realizacją usługi wdrożenia Systemu; * spowodowanych aktualizacjami Systemu. |
| WG10 | Wykonawca musi informować Zamawiającego o dostępnych aktualizacjach i poprawkach Systemów |
| WG11 | Zgłaszający, w przypadku wystąpienia dysfunkcji przesyła do Wykonawcy przy pomocy środków komunikacji formularz zgłoszenia wystąpienia Dysfunkcji. W Zgłoszeniu powinny być wypełnione wszystkie obligatoryjne pola formularza, a opis sytuacji prowadzącej do wystąpienia błędu lub awarii powinien umożliwiać jej odtworzenie przez zespół serwisowy Wykonawcy. Jeżeli odtworzenie błędu nie będzie możliwe w środowisku Wykonawcy, wówczas zdiagnozuje on błąd w środowisku Zamawiającego, ale terminy świadczenia usług gwarancyjnych ulegają wydłużeniu o czas oczekiwania na dostęp do środowiska Zamawiającego. |
| WG12 | Wykonawca zobowiązany jest do potwierdzenia w ciągu 4 godzin w czasie okna dostępności usługi serwisowej przyjęcie Zgłoszenia oraz jego klasyfikację – nie dotyczy Zgłoszeń Krytycznych. Potwierdzenie zostanie wysłane przez Wykonawcę do zgłaszającego.  Zgłoszenia Krytyczne Wykonawca będzie realizował niezwłocznie po ich otrzymaniu. |
| WG13 | Wykonawca zapewnia dostosowanie do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie, Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie. |
| WG14 | Zgłoszenia będą klasyfikowane zgodne ze słownikiem pojęć, zawartym w Załączniku nr 6 do Umowy, przez Zamawiającego w uzgodnieniu z Wykonawcą. |
| WG15 | Wykonawca zobowiązany jest do usunięcia dysfunkcji w terminach wymienionych w pkt 7 procedury podejmowania prac serwisowych zawartej w Załączniku nr 6 do Umowy.. |
| WG16 | W każdym przypadku Zgłaszający i Wykonawca mogą uzgodnić inny czas dostarczenia rozwiązania niż określono w warunkach gwarancji. W takim przypadku niezbędne jest potwierdzenie ustalonego terminu w formie pisemnej, faksem lub e-mailem. |
| WG17 | Terminy naprawy sprzętu są uzależnione od funkcji dostarczonego sprzętu i są podane w części specyfikacji sprzętu. |
| WG18 | W ramach świadczonej usługi chmurowej Wykonawca musi zapewnić usługę backupu opisaną w instrukcji backupu i archiwizacji stworzonej wspólne z Zamawiającym. |

# Zastrzeżenie równoważności rozwiązań

W niniejszym dokumencie przedstawione są wymagania dotyczące zamawianego sprzętu, oprogramowania i usług. Z uwagi na to, że art. 30 ust. 5 ustawy prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę, jako tego, który jest zobowiązany wykazać, że rozwiązanie równoważne spełniają wymagania Zamawiającego wynikające z Opisu Przedmiotu Zamówienia. Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności oferowanych produktów z wymogami specyfikacji, w przypadku wątpliwości oferowanego rozwiązania.

Sprawdzenie to, będzie polegać na przeprowadzeniu testów w warunkach produkcyjnych.

Zamawiający może w każdym momencie realizacji projektu zażądać zaprezentowania wszystkich funkcjonalności wymaganych w SIWZ i zaoferowanych w ofercie, w terminach wymagalnych wynikających z przyjętego harmonogramu. Prezentacja i akceptacja funkcjonalności wersji systemu będzie wykonana w miejscu wskazanym przez Zamawiającego.

# Spis tabel:

[Tabela 1. Ramowy wykaz ilości minimalnych dostarczanych rozwiązań do poszczególnych Partnerów Projektu 5](#_Toc498974352)

[Tabela 2 Wykaz lokalizacji partnerów biorących udział w Projekcie 12](#_Toc498974353)

[Tabela 3 Ramowe zestawienie zakresu przedmiotu zamówienia 12](#_Toc498974354)

[Tabela 4 Wymagania ogólne dotyczące dostarczanego rozwiązania 16](#_Toc498974355)

[Tabela 5 Wymagania ogólne dot. dostarczanego sprzętu 17](#_Toc498974356)

[Tabela 6 Wymagania minimalne dotyczące Routera CE 18](#_Toc498974357)

[Tabela 7 Wymagania minimalne dotyczące Serwera - wariant I 21](#_Toc498974358)

[Tabela 8 Wymaganie minimalne dotyczące serwera - wariant II 23](#_Toc498974359)

[Tabela 9 Wymagania minimalne dotyczące macierzy dyskowej w zasobach lokalnych 24](#_Toc498974360)

[Tabela 10 Wymagania minimalne dotyczące komputera stacjonarnego z monitorem 27](#_Toc498974361)

[Tabela 11 Wymagania minimalne dotyczące komputera przenośnego typu laptop 28](#_Toc498974362)

[Tabela 12 Wymagania minimalne dotyczące parametrów skanera małego 28](#_Toc498974363)

[Tabela 13 Wymagania minimalne dotyczące parametrów skanera dużego 29](#_Toc498974364)

[Tabela 14 Wymagania minimalne dotyczące parametrów drukarki etykiet 30](#_Toc498974365)

[Tabela 15 Wymagania minimalne dotyczące parametrów skanerów kodów kreskowych 30](#_Toc498974366)

[Tabela 16 Wymagania minimalne dotyczące przełączników sieciowych 31](#_Toc498974367)

[Tabela 17 Wymagania minimalne dotyczące prac w ramach modernizacji sieci LAN 38](#_Toc498974368)

[Tabela 18 Przewidywane miejsca instalacji punktów WiFi 39](#_Toc498974369)

[Tabela 19 Wymagania minimalne dotyczące parametrów punktów WiFi 40](#_Toc498974370)

[Tabela 21 Zakres prac w ramach wdrożenia EOD i integracji 43](#_Toc498974371)

[Tabela 22 Parametry minimalne wdrożonych formularzy elektronicznych 45](#_Toc498974372)

[Tabela 23 Lista formularzy elektronicznych wdrażanych u poszczególnych Partnerów Projektu 46](#_Toc498974373)

[Tabela 24 Parametry minimalne SUE 48](#_Toc498974374)

[Tabela 25 Parametry minimalne modułu konta klienta 52](#_Toc498974375)

[Tabela 26 Wymagania minimalne dot. modułu elektronicznego biura interesanta 53](#_Toc498974376)

[Tabela 27 Wymagania minimalne dot. modułu Płatności 0n-line 55](#_Toc498974377)

[Tabela 28 Parametry minimalne Centralnej Szyny Danych 57](#_Toc498974378)

[Tabela 29 Parametry minimalne centralnej szyny danych oraz minimalny zakres usług bezpieczeństwa transferu danych 58](#_Toc498974379)

[Tabela 30 Minimalny zakres integracji SUE z SB 75](#_Toc498974380)

[Tabela 31 Minimalny zakres prac wdrożeniowych 75](#_Toc498974381)

[Tabela 32 Minimalny zakres szkoleń dla Administratorów 77](#_Toc498974382)

[Tabela 33 Parametry minimalne dla dostarczonej dokumentacji 78](#_Toc498974383)

[Tabela 34 Minimalny zakres prac świadczonych w ramach usługi wsparcia i serwisu 79](#_Toc498974384)

1. Na całość rozwiązania od momentu podpisania ostatniego Protokołu Odbioru Końcowego Zakresów od 1 do 6. [↑](#footnote-ref-1)