

# OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Podniesienie poziomu bezpieczeństwa sieci teleinformatycznej używanej w ramach Państwowej Inspekcji Sanitarnej poprzez rozbudowę rządowej sieci teletransmisyjnej GovNet		
Wnioskodawca	Minister Spraw Wewnętrznych i Administracji		
Beneficjent	Ministerstwo Spraw Wewnętrznych i Administracji		
Partnerzy	Główny Inspektorat Sanitarny		
Źródło finansowania	Środki UE: Program Operacyjny Polska Cyfrowa, Oś Priorytetowa V (POPC REACT-EU)		
Całkowity koszt projektu	60 000 000,00 zł		
Planowany okres realizacji projektu	05-2021 do 12-2023		
Osoba kontaktowa	Tomasz Świątkowski	tomasz.swiatkowski@mswia.gov.pl	783934220

## 1. POWODY PODJĘCIA PROJEKTU

### 1.1. Identyfikacja problemu i potrzeb

W związku z działaniami związanymi z digitalizacją GIS (doposażenie w laptopy i smartfony, budowa SEPIS oraz uruchomienie ogólnokrajowej infolinii dla obywateli), w celu zapewnienia bezpieczeństwa przyjętych rozwiązań konieczne jest podjęcie działań w zakresie transmisji oraz ochrony przesyłanych i przetwarzanych danych. W ramach rozbudowy rządowej sieci GovNet, na potrzeby stacji sanitarno-epidemiologicznych, wydzielona zostanie dedykowana sieć VPN/LAN. W ramach projektu zakupione zostaną telefony VoIP oraz moduł bezpieczeństwa dla usług dostępu do Internetu. Rezultatem rozbudowy sieci GovNet będzie utworzenie nowych węzłów szkieletowych (agregacyjnych) oraz powiatowych, pozwalających w przyszłości na połączenie administracji rządowej oraz samorządowej za pomocą jednolitej sieci teletransmisyjnej opartej na technologii MPLS. Każdy nowoutworzony węzeł sieci GovNet wyposażony zostanie w urządzenia sieciowe (routery) a istniejących 8 węzłów zostanie doposażonych w siłownie telekomunikacyjne wraz z bateriami. Wszystkie węzły połączone zostaną łączami dostępowymi o dużej przepustowości (m. in. zwiększona zostanie przepustowość łączy w istniejących węzłach). W celu nadzoru nad siecią wdrożony zostanie dedykowany system do zarządzania i monitorowania sieci oraz system do paszportyzacji sieci. Ze względu na krytyczny charakter sieci oraz jej znaczenie dla bezpieczeństwa zarówno pod względem infrastruktury, jak i świadczonych za jej pośrednictwem usług, przygotowane zostaną plany ciągłości działania sieci. Po realizacji projektu do rozbudowanej sieci GovNet będą mogły podłączyć się inne instytucje rządowe, pozarządowe oraz samorządowe. Całe rozwiązanie ograniczy zagrożenia w użytkowaniu sieci, pozwoli wdrożyć nowoczesne mechanizmy bezpieczeństwa teleinformatycznego, wdroży wysokie SLA oraz zapewni dostęp do szeregu usług publicznych świadczonych za pośrednictwem sieci GovNet (m. in. systemy Rejestrów Państwowych, do których należą: PESEL, RDO, RSC, RDK, SOP i CRS).

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Główny Inspektorat	Brak jednej, bezpiecznej sieci	Główny Inspektorat

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Sanitarny	teletransmisyjnej łączącej wszystkie jednostki GIS, dzięki której byłaby możliwość przesyłania danych w sposób jednolity, zapewniający zachowanie ich integralności, rozliczalności i poufności.	Sanitarny 16 Wojewódzkich Stacji Sanitarno – Epidemiologicznych. 318 Powiatowych Stacji Sanitarno - Epidemiologicznych. 10 Granicznych Stacji Sanitarno - Epidemiologicznych. Łącznie blisko 17 000 pracowników.
Administracja rządowa	Brak jednej, dedykowanej, odseparowanej sieci realizującej usługi transmisji danych na rzecz jednostek szczebla rządowego.	Rozwiązanie horyzontalne dla całej administracji rządowej: 15 ministerstw, 16 urzędów wojewódzkich, 3084 jednostek podległych.
Administracja samorządowa	Brak jednej, dedykowanej, odseparowanej sieci realizującej usługi transmisji danych na rzecz jednostek szczebla samorządowego.	Rozwiązanie horyzontalne dla całej administracji samorządowej w: 314 powiatach, 66 miastach na prawach powiatów.
Obywatele RP	Utrudniony kontakt z Państwową Inspekcją Sanitarną w sprawach obsługiwanych przez stacje sanitarno-epidemiologiczne.	38 mln

## 1.2. Opis stanu obecnego

Obecnie wykorzystywane w jednostkach PIS rozwiązanie w zakresie usługi VoIP realizowane jest w oparciu o technologię LTE. Rozwiązanie to zostało wdrożone w krótkim czasie na potrzeby łączności PSSE i WSSE z obywatelami w czasie trwającej pandemii COVID-19. Głównym założeniem wdrożonego rozwiązania było usprawnienie komunikacji do skutecznej walki z epidemią i jego wykorzystanie m.in. do przeprowadzania wywiadów epidemiologicznych z osobami zakażonymi wirusem, aby poprzez obejmowanie osób z kontaktu kwarantanną skutecznie przerwać łańcuch zakażeń. Obecnie brak jest centralizacji danych i wymiany informacji pomiędzy stacjami sanitarno-epidemiologicznymi. Nie ma jednego miejsca dostępu do bieżących dokumentów, wytycznych, procedur, co powoduje rozbieżności w podejściu do pracy. W celu ujednolicenia procesów i oparcia ich o rozwiązania informatyczne niezbędna jest, poza budową scentralizowanego systemu informatycznego (SEPIS), rozbudowa wewnętrznej sieci LAN oraz podłączenie stacji sanitarno-epidemiologicznych do bezpiecznej sieci GovNet, która stworzy możliwość wymiany informacji, w codziennej pracy, w sposób jednolity. W chwili obecnej rządowa sieć teletransmisyjna GovNet, która w przyszłości zostanie wykorzystana do poprawy bezpieczeństwa rozwiązań i usług realizowanych przez Państwową Inspekcję

Sanitarną, obejmuje swoim zasięgiem aglomerację warszawską (ministerstwa, służby, instytucje) a także wszystkie urzędy wojewódzkie. Łącznie funkcjonuje 116 węzłów sieci GovNet na terenie całej RP. W ramach sieci GovNet udostępniane są kluczowe usługi takie jak: SRP, CEPiK, wideokonferencje, telefonia tradycyjna i VoIP na rzecz administracji rządowej. Jednostki administracji rządowej oraz samorządowej RP korzystają z usług różnych operatorów telekomunikacyjnych, a także różnych mediów transmisyjnych, co sprawia, że pokrycie sieciowe poszczególnych resortów jest niespójne i nieskalowalne, nieefektywne ekonomicznie oraz zwiększa ryzyko związane z bezpieczeństwem informacji.

## 2. EFEKTY PROJEKTU

### 2.1. Cele i korzyści wynikające z projektu

<b>Cel - 1</b>	Budowa sieci VPN/LAN dla stacji sanitarno-epidemiologicznych.
<b>Cel strategiczny</b>	<p>Program Zintegrowanej Informatyzacji Państwa:  Stworzenie spójnego, logicznego i sprawnego systemu informacyjnego państwa, zapewniającego przejrzystość funkcjonowania administracji i dostarczającego na poziomie wewnątrzpaństwowym i europejskim usługi kluczowe dla obywateli i przedsiębiorców, w sposób efektywny kosztowo i jakościowo oraz zapewnienie interoperacyjności istniejących oraz nowych systemów teleinformatycznych administracji.</p> <p>Program Zintegrowanej Informatyzacji Państwa na lata 2014-2022  - Modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami</p> <p>4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office)</p> <p>4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej</p>
<b>Korzyść:</b>	<ol style="list-style-type: none"> <li>1. Wzrost poziomu bezpieczeństwa działania stacji sanitarno-epidemiologicznych w zakresie m.in. transmisji danych i ochrony prywatności.</li> <li>2. Minimalizacja zagrożeń w użytkowaniu wewnętrznej sieci Państwowej Inspekcji Sanitarnej.</li> <li>3. Wdrożenie nowoczesnych mechanizmów bezpieczeństwa teleinformatycznego.</li> <li>4. Zapewnienie dostępu do szeregu kluczowych usług publicznych świadczonych za pośrednictwem rządowej sieci teletransmisyjnej GovNet, w tym Systemu Rejestrów Państwowych, dzięki czemu uproszczona zostanie obsługa procesów m. in. w Państwowej Inspekcji Sanitarnej.</li> <li>5. Ograniczenie kosztów ponoszonych przez PSSE z tytułu wykorzystywania usług VoIP w technologii LTE.</li> </ol>
<b>KPI:</b>	<p>KPI 1: Liczba stacji sanitarno-epidemiologicznych wpiętych w wewnętrzną sieć VPN/LAN.</p> <p>KPI 2: Liczba użytkowników korzystających ze zmodernizowanej w ramach projektu telefonii VoIP.</p> <p>KPI 3: Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych.</p> <p>KPI 4: Liczba osób objętych wsparciem w zakresie zwalczania lub przeciwdziałania skutkom pandemii COVID-19.</p>

	KPI 5: Liczba podmiotów objętych wsparciem w zakresie zwalczania lub przeciwdziałania skutkom pandemii COVID-19.
<b>Wartość aktualna i docelowa KPI:</b>	<p>KPI 1: 0 jednostek Państwowej Inspekcji Sanitarnej</p> <p>KPI 2: 0 użytkowników</p> <p>KPI 3: 0 użytkowników</p> <p>KPI 4: 0 użytkowników</p> <p>KPI 5: 0 jednostek Państwowej Inspekcji Sanitarnej</p> <p>KPI 1: 345 jednostek Państwowej Inspekcji Sanitarnej</p> <p>KPI 2: 8000 użytkowników</p> <p>KPI 3: 4000 użytkowników</p> <p>KPI 4: 8000 użytkowników</p> <p>KPI 5: 345 jednostek Państwowej Inspekcji Sanitarnej</p>
<b>Metoda pomiaru KPI</b>	<p>1. Protokół odbioru etapu, rocznie.</p> <p>2. Raport końcowy projektu, rocznie.</p> <p>3. Protokół odbioru szkolenia, rocznie.</p>
<b>Cel - 2</b>	Zwiększenie zasięgu kluczowych usług, takich jak dostęp Systemu Rejestrów Państwowych, CEPiK, wideokonferencje, telefonia tradycyjna i VoIP.
<b>Cel strategiczny</b>	<p>Program Zintegrowanej Informatyzacji Państwa:</p> <p>Stworzenie spójnego, logicznego i sprawnego systemu informacyjnego państwa, zapewniającego przejrzystość funkcjonowania administracji i dostarczającego na poziomie wewnątrz krajowym i europejskim usługi kluczowe dla obywateli i przedsiębiorców, w sposób efektywny kosztowo i jakościowo oraz zapewnienie interoperacyjności istniejących oraz nowych systemów teleinformatycznych administracji.</p> <p>Program Zintegrowanej Informatyzacji Państwa na lata 2014-2022</p> <ul style="list-style-type: none"> <li>- Modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami</li> </ul> <p>4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office)</p> <p>4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej</p> <p>Długookresowa Strategia Rozwoju Kraju Polska 2030</p> <ul style="list-style-type: none"> <li>- Cel 10 – Stworzenie sprawnego państwa jako modelu działania administracji publicznej</li> </ul>
<b>Korzyść:</b>	Zapewnienie dostępu do ustandaryzowanej infrastruktury komunikacyjnej, umożliwiającej teletransmisję danych dla szerokiego grona odbiorców szczebla rządowego i samorządowego w ramach kluczowych usług mających wpływ na bezpieczeństwo Państwa.
<b>KPI:</b>	<p>KPI 1: Liczba uruchomionych węzłów GovNet.</p> <p>KPI 2: Liczba uruchomionych siłowni telekomunikacyjnych.</p> <p>KPI 3: Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 (CV 4).</p> <p>KPI 4: Wartość sprzętu IT oraz oprogramowania/licencji finansowanych w odpowiedzi na COVID-19 dla sektora ochrony zdrowia (CV 4b).</p> <p>KPI 5: Wartość wydatków kwalifikowalnych przeznaczonych na działania związane z pandemią COVID-19.</p>
<b>Wartość</b>	<p>KPI 1: 116 węzłów</p> <p>KPI 2: 11 siłowni telekomunikacyjnych</p>

<b>aktualna i docelowa KPI:</b>	telekomunikacyjnych KPI 3: 0,00 zł KPI 4: 0,00 zł KPI 5: 0,00 zł KPI 1: 461 węzłów KPI 2: 19 siłowni telekomunikacyjnych KPI 3: 30.000.000,00 zł KPI 4: 30.000.000,00 zł KPI 5: 60.000.000,00 zł
<b>Metoda pomiaru KPI</b>	1. Protokół odbioru etapu, rocznie. 2. Raport końcowy projektu, rocznie. 3. Dokumenty potwierdzające zakup sprzętu i licencji, rocznie.

## 2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi

## 2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

## 2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
System zarządzania i monitorowania sieci	05-2022
Telefony VoIP dla GIS	08-2022
Zmodernizowane łącza dostępowe w istniejących 17 węzłach wojewódzkich	09-2022
Siłownie telekomunikacyjne wraz z bateriami	10-2022
Urządzenia sieciowe – routery	10-2022
System do paszportyzacji sieci	04-2023
Łącza dostępowe w nowych 345 lokalizacjach	10-2023
Węzły szkieletowe (agregacyjne) sieci GovNet w 17 lokalizacjach	10-2023
Węzły dostępowe sieci GovNet w nowych 345 lokalizacjach (powiatowe)	10-2023
Wewnętrzna sieć LAN dla GIS	11-2023
Moduł bezpieczeństwa wraz z usługą dostępu do sieci Internet	11-2023
Plany ciągłości działania dla sieci GovNet	12-2023
Przeprowadzone szkolenia dla użytkowników	12-2023

Nazwa produktu	Planowana data wdrożenia
Przygotowane materiały informacyjno - promocyjne	12-2023
Dokumentacja powykonawcza i eksploatacyjna	12-2023

### 3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Przygotowany i zaakceptowany Projekt Techniczny rozbudowy sieci GovNet	2021-12-31
Uruchomiony system zarządzania i monitorowania sieci	2022-05-31
Dostarczenie i konfiguracja urządzeń sieciowych potwierdzona pozytywnym wynikiem testów akceptacyjnych	2022-10-31
Dostarczenie i montaż siłowni telekomunikacyjnych wraz z bateriami potwierdzone protokołem odbioru bez zastrzeżeń	2022-10-31
Uruchomione produkcyjnie węzły dostępne w 115 wybranych jednostkach GIS (Etap I GIS)	2023-02-28
Uruchomiony system do paszportyzacji sieci	2023-04-30
Uruchomione produkcyjnie węzły dostępne w 115 wybranych jednostkach GIS (Etap II GIS)	2023-07-31
Uruchomione produkcyjnie węzły dostępne w 115 wybranych jednostkach GIS (Etap III GIS)	2023-10-31
Uruchomione produkcyjnie wszystkie węzły szkieletowe i dostępne, będące przedmiotem projektu	2023-12-31

### 4. KOSZTY

#### 4.1. Koszty ogólne projektu wraz ze sposobem finansowania

<b>Całkowity koszt projektu (netto oraz brutto), w tym</b>	Netto 48 780 487,81 zł Brutto 60 000 000,00 zł	
<b>Procent dofinansowania ze środków UE (brutto)</b>	100%	
<b>Procent środków z budżetu państwa (brutto)</b>		
<b>Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)</b>	2021	Netto 162 601,63 zł Brutto 200 000,00 zł
	2022	Netto 24 308 943,09 zł Brutto 29 900 000,00 zł
	2023	Netto 24 308 943,09 zł Brutto 29 900 000,00 zł

## 4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Koszty zakupu gotowych rozwiązań informatycznych/programistycznych, koszty oprogramowania standardowego.	4 500 000,00 zł	Zakup, konfiguracja i wdrożenie systemu do zarządzania i monitorowania sieci, system do paszportyzacji sieci.
Infrastruktura	Zakup sprzętu sieciowego, sprzętu telekomunikacyjnego oraz łączы dostępowych i sieci Internet.	46 000 000,00 zł	Zakup sprzętu sieciowego, telefonów VoIP (rozbudowa obecnie funkcjonującej w jednostkach Państwowej Inspekcji Sanitarnej telefonii VoIP o dodatkowe telefony - 4.000 szt.), siłowni telekomunikacyjnych oraz łączы, koniecznych do realizacji założonego celu projektu.
Koszty UX i grafiki			
Bezpieczeństwo	Moduł bezpieczeństwa dla usługi Internet, plany ciągłości działania i audyt bezpieczeństwa.	2 500 000,00 zł	Zakup modułu bezpieczeństwa dla sieci Internet, konieczność sporządzenia planów ciągłości działania oraz przeprowadzenia audytu bezpieczeństwa wdrażanego rozwiązania.
Wydajność rozwiązań			

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Szkolenia	Koszty szkoleń zespołu projektowego i użytkowników końcowych projektu.	500 000,00 zł	Nakłady niezbędne do podniesienia kompetencji pracowników biorących udział w realizacji założonych celów projektu.
Działania informacyjno-promocyjne	Koszty wszystkich działań informacyjno-promocyjnych.	500 000,00 zł	Realizacja celów projektu wymaga wprowadzenia skutecznych działań informacyjnych i promocyjnych, w szczególności w jednostkach administracji samorządowej.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszty zespołu wspomagającego realizację projektu, koszty zespołu wykonującego merytoryczne zadania projektu, analizy, nadzór merytoryczny, usługi wspomagające realizację projektu (doradcze i eksperckie).	6 000 000,00 zł	Pozycja kosztowa zawierająca wynagrodzenia osób zaangażowanych w realizację projektu.

#### 4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	50 890 000,00 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2024	10 178 000,00 zł (brutto) (8 274 796,75 zł netto)	krajowe środki publiczne - budżet państwa
	2025	10 178 000,00 zł (brutto) (8 274 796,75 zł netto)	krajowe środki publiczne - budżet państwa
	2026	10 178 000,00 zł (brutto) (8 274 796,75 zł netto)	krajowe środki publiczne - budżet państwa
	2027	10 178 000,00 zł (brutto) (8 274 796,75 zł netto)	krajowe środki publiczne - budżet państwa



	2028	10 178 000,00 zł (brutto) (8 274 796,75 zł netto)	krajowe środki publiczne - budżet państwa
--	------	--	---

#### 4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- będą powodować konieczność przyznania dodatkowych kwot

### 5. GŁÓWNE RYZYKA

#### 5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Utrudnienia w dostawach sprzętu, możliwości wykonania instalacji w obiektach posadowienia węzłów.	Duża	Średnie	Redukowanie: Przygotowany z wyprzedzeniem harmonogram dostaw i instalacji sprzętu. Przygotowanie zamówienia publicznego z odpowiednim wyprzedzeniem. Wczesne rozeznanie rynku w zakresie możliwych terminów dostaw.
Utrudnienia w pracach budowlanych łącz dostępowych (warunki atmosferyczne, uzyskanie stosownych zezwoleń).	Duża	Średnie	Redukowanie: Odpowiednie wczesne wystąpienie o stosowne zezwolenia. Przygotowany i uzgodniony harmonogram prac. Ścisła współpraca z wykonawcą. Dostosowanie harmonogramu do przewidywanych warunków atmosferycznych.
Brak doświadczenia i umiejętności w zakresie dużych projektów związanych z rozbudową i wdrażaniem rozwiązań sieciowych.	Średnia	Średnie	Redukowanie: Pozyskanie kompetentnych osób do zespołu lub zapewnienie wsparcia przez zewnętrznych ekspertów. Przekazywanie między pracownikami wiedzy merytorycznej umożliwiającej zaspokojenie braków kadrowych. Korzystanie z doświadczeń podobnych projektów. Bieżące prowadzenie dokumentacji projektowej.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Wzrost kosztów realizacji projektu wynikający z wahan kursu walut.	Średnia	Niskie	Unikanie: Zawarcie w umowie z wykonawcą klauzul w zakresie zmiany wynagrodzenia za realizację przedmiotu zamówienia.
Przedłużające się restrykcje związane z ograniczaniem skutków epidemii COVID-19 w zakresie bezpośrednich kontaktów międzyludzkich wpływające na efektywność pracy zespołów.	Średnia	Średnie	Redukowanie: Organizacja pracy zdalnej. Bieżący monitoring sytuacji epidemiologicznej i dostosowanie pracy w zespole projektowym do stanu aktualnego.

## 5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak zrozumienia zakresu projektu oraz płynących z jego realizacji korzyści.	Mała	Niskie	Redukowanie: Promowanie wiedzy o projekcie i korzyściach płynących z jego realizacji.
Wzrost kosztów utrzymania trwałości projektu, do którego mogą się przyczynić w przyszłości zmiany przepisów prawa polskiego i/ lub europejskiego.	Średnia	Niskie	Unikanie: Wypracowanie aktu regulującego funkcjonowanie rządowej sieci teletransmisyjnej GovNet.
Trudności w utrzymywaniu efektów projektu po upływie okresu gwarancyjnego przez innego	Średnia	Średnie	Unikanie: Zawarcie w umowie z wykonawcą klauzul gwarantujących przekazanie dokumentacji oraz wszystkich majątkowych praw autorskich.

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
przedsiębiorcę niż wykonawca wyłoniony podczas realizacji projektu.			

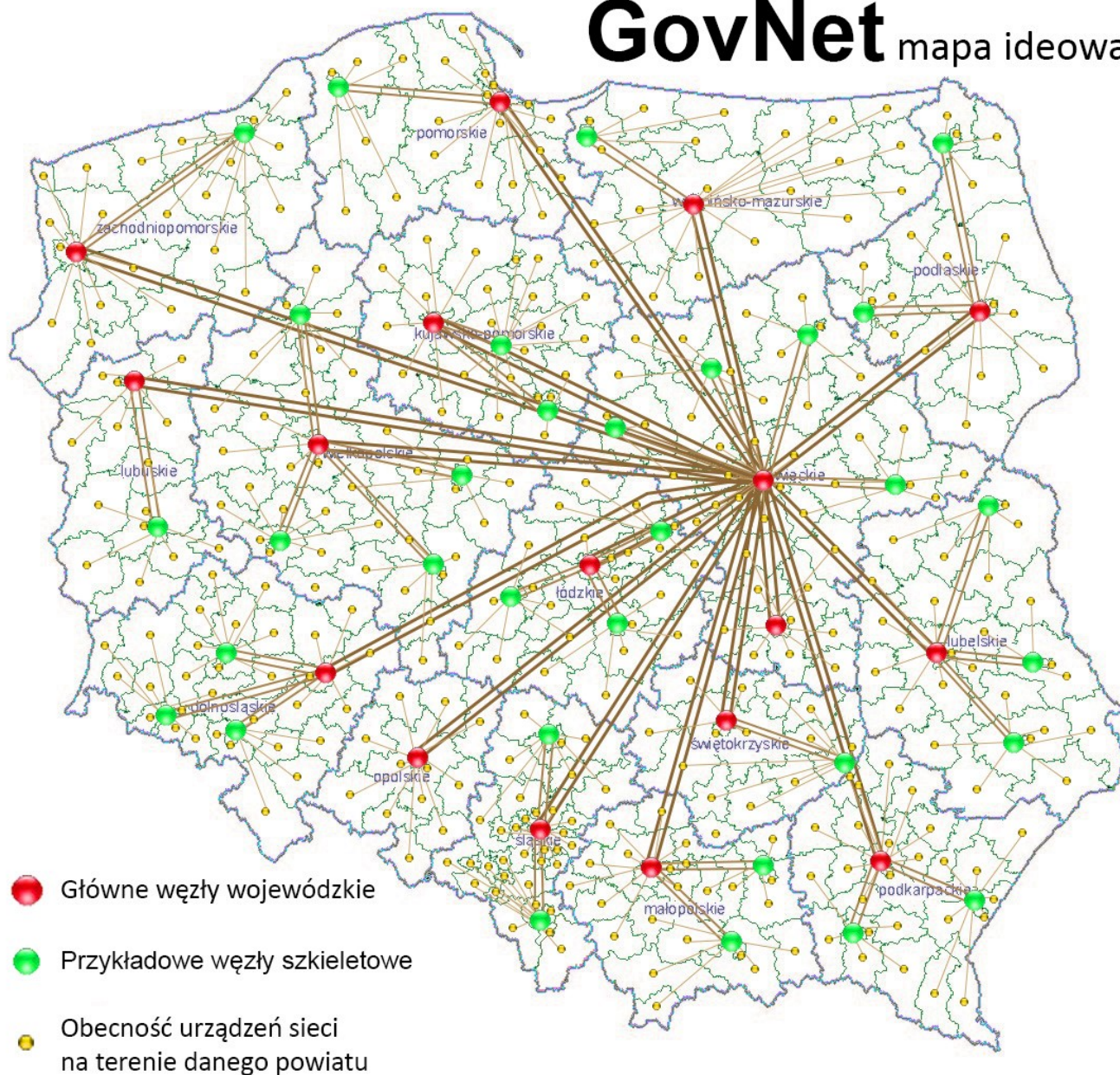
## 6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej	TAK/NIE		
2	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne	TAK/NIE		
3	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	TAK/NIE		
4	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	TAK/NIE		

## 7. ARCHITEKTURA

### 7.1. Widok kooperacji aplikacji

# GovNet mapa ideowa



## Lista systemów wykorzystywanych w projekcie

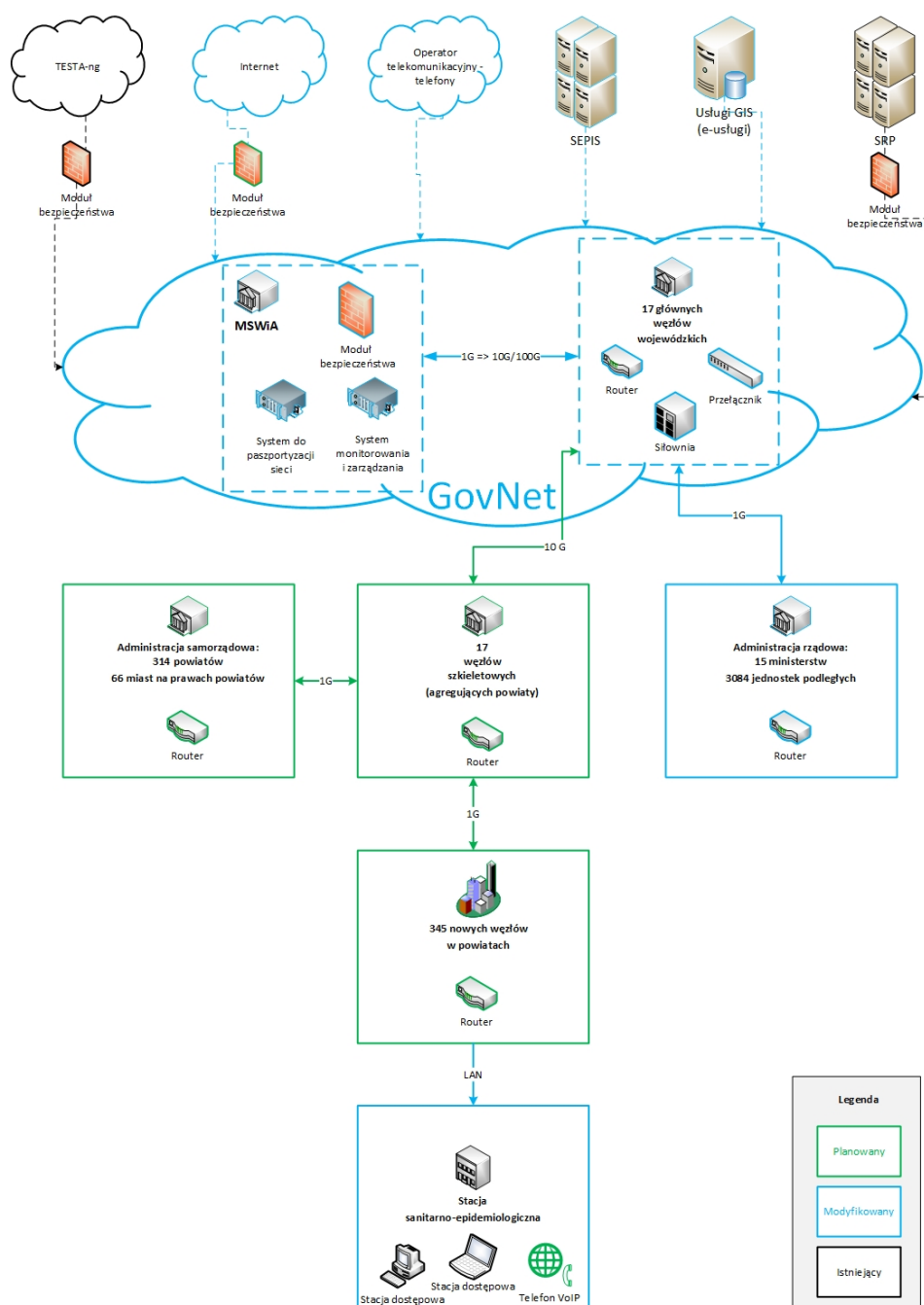
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	nie dotyczy	nie dotyczy	nie dotyczy	Planowany	nie dotyczy

## Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
-----	-----------------	-----------------	----------------------------	-----------------------	-----------------	----------------

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy	nie dotyczy

## 7.2. Kluczowe komponenty architektury rozwiązania



## 7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Urządzenia Juniper (technologia MPLS) – urządzenia będące w chwili obecnej w gestii MSWiA wraz z systemem zarządzania i monitoringu (sieć GovNet jest siecią homogeniczną sprzętowo). Urządzenia telekomunikacyjne - technologia VoIP.
2.	Sieć i bezpieczeństwo	GovNet - sieć wydzielona, zarządzana przez MSWiA poprzez dedykowany system, szyfrowanie kanałów komunikacji.
3.	Standardy wymiany danych	
4.	Systemy operacyjne serwerowe	Linux, Windows Server.
5.	Bazy danych	
6.	Serwery aplikacji	
7.	Portale	
8.	Inne	Junos Space.

## 7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/NIE

## 7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...]) (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

- system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI

Rozbudowa sieci teletransmisyjnej GovNet nie podlega wymogom KRI, ponieważ nie tworzy zbiorów o charakterze rejestrów publicznych, ani nie przewiduje zasilania innych rejestrów publicznych.

W Ministerstwie Spraw Wewnętrznych i Administracji wprowadzono System Zarządzania Bezpieczeństwem Informacji, zarządzeniem nr 7 Ministra Spraw Wewnętrznych i Administracji z dnia 20 lutego 2017 r. w sprawie Systemu Zarządzania Bezpieczeństwem Informacji w Ministerstwie Spraw Wewnętrznych i Administracji.

Podejmowane działania z zakresu zarządzania bezpieczeństwem informacji obejmują m.in:

1. Zapewnianie aktualizacji regulacji wewnętrznych w przypadku zmian w otoczeniu.
2. Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania.
3. Stosowanie środków organizacyjnych zapewniających, że osoby zaangażowane w proces przetwarzania informacji: 1/ posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do ich stanowiska i sprawowanych obowiązków; 2/ mają zapewnione szkolenia w zakresie zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa oraz stosowania środków zapewniających bezpieczeństwo informacji.
4. Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.

5. Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.
6. Zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji (takie zapisy znajdują się w umowach z dostawcami sprzętu i oprogramowania na potrzeby projektu).
7. Ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.
8. Okresowo zapewniony będzie audyt wewnętrzny w zakresie bezpieczeństwa informacji, w tym dotyczący nowo wdrożonego systemu/sieci.

~~-dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~