

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

| | | | |
|-------------------------------------|--|------------------------|-----------|
| Tytuł projektu | Podłączenie 385 nowych podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem (system S46) oraz dalszy rozwój tego systemu | | |
| Wnioskodawca | Minister Cyfryzacji | | |
| Beneficjent | NASK PIB | | |
| Partnerzy | | | |
| Źródło finansowania | Krajowy Plan Odbudowy i Zwiększania Odporności, działanie C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo; budżet państwa, część budżetowa - w takcie ustaleń; | | |
| Całkowity koszt projektu | 41 741 692,14 zł | | |
| Planowany okres realizacji projektu | 01-2024 do 06-2026 | | |
| Osoba kontaktowa | Daniel Wachnik | daniel.wachnik@nask.pl | 885457494 |

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Infrastruktura teleinformatyczna państwa – co szczególnie unaocznili okres pandemii – jest kluczową infrastrukturą dla gospodarki narodowej, administracji, zdrowia publicznego, kultury itp. Zatem jej ochrona powinna być traktowana jako ochrona istotnego interesu bezpieczeństwa państwa. Ochrona ta jest realizowana przez systemy zapewniające cyberbezpieczeństwo różnych podmiotów – na poziomie lokalnym. Skuteczne kierowanie ochroną cyberbezpieczeństwa wymaga także działań perymetrycznych ponadlokalnych, regionalnych, a także centralnych. Uruchomiony 1 stycznia 2021 roku system S46 ma za zadanie zarządzanie cyberbezpieczeństwem na poziomie państwa – realizując w ten sposób efektywne działanie krajowego systemu cyberbezpieczeństwa (KSC). Z punktu widzenia Państwa, współdziałanie podmiotów krajowego systemu cyberbezpieczeństwa oraz udostępnianie jednostkom krajowym informacji o obrazie sytuacyjnym cyberbezpieczeństwa, ich ostrzeganie, jak i prewencyjne wskazywanie podatności jest jednym z podstawowych i istotnych zagadnień zwiększających holistycznie odporności systemów informacyjnych RP na cyberzagrożenia. Istotnym problemem jaki się pojawia w działaniu systemu S46 jest zapewnienie dostępu do niego szerokim grupom ważnych odbiorców – tworzących wspólnie spójny obraz cyberbezpieczeństwa w Polsce oraz nadążanie za wyzwaniami w niezwykle szybko zmieniającym się otoczeniu cyfrowym.

Szczegółowe problemy, jakie zostały zidentyfikowane i które mają być rozwiązane przez realizację przedmiotowego projektu przedstawia tabela.

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|-----------------------------|--|--------------------------|
| Operatorzy Usług Kluczowych | <ul style="list-style-type: none">Brak kompletnej, jednolitej, stabilnej i wiarygodnej metody wymiany informacji | 385 |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|---|--|--------------------------|
| (nowelizacja ustawy o KSC wprowadzi pojęcie podmiotu kluczowego, które obejmie Operatorów Usług Kluczowych) | <p>między podmiotami krajowego systemu cyberbezpieczeństwa i CSIRT;</p> <ul style="list-style-type: none"> Wysoki początkowy koszt podłączenia do s46; Nieotrzymywanie ostrzeżeń o zagrożeniach i zagregowanej informacji o podatnościach – w sposób systemowy, zintegrowany – a przez to skuteczny. | |
| Przedstawiciele podłączanych do S46 Operatorów Usług Kluczowych (zgodnie z aktualnie obowiązującą ustawą o KSC) | <ul style="list-style-type: none"> Niewystarczający poziom wiedzy pracowników podłączanych jednostek o sposobie funkcjonowania systemu S46 | 770 |
| Podmioty kluczowe i ważne, podlegające procesowi samorejestracji na podstawie przepisów NIS2, z wyłączeniem Operatorów Usług Kluczowych | <ul style="list-style-type: none"> Brak centralnego mechanizmu identyfikacji, samorejestracji, klasyfikowania i aktualizacji informacji o podmiotach krajowego systemu cyberbezpieczeństwa; Brak kompletnej, jednolitej, stabilnej i wiarygodnej metody wymiany informacji; Nieotrzymywanie ostrzeżeń o zagrożeniach i zagregowanej informacji o podatnościach – w sposób systemowy, zintegrowany – a przez to skuteczny. | 38147 |
| Ministerstwo Cyfryzacji | <ul style="list-style-type: none"> Niewystarczające w stosunku do potrzeb liczby podmiotów podłączonych do s46 powoduje niepełny obraz sytuacyjny cyberbezpieczeństwa oraz ryzyka dynamicznego świadczonych usług – w szczególności dla jednostek uczestniczących w zintegrowanym systemie zarządzania kryzysowego Spodziewane problemy z dostępnością systemu S46, dla nowopodłączanych użytkowników ze względu na niedoskalowanie usług centralnych. Niewystarczające mechanizmy komunikacyjne w systemie S46 w stosunku do potrzeb zgłaszanych przez użytkowników;; Brak mechanizmu samorejestracji podmiotów, wprowadzania i aktualizacji danych wymaganych w ramach NIS2. | 1 |

1.2. Opis stanu obecnego

Zobowiązanie do zbudowania systemu S46 jako strategicznego przedsięwzięcia zostało wprowadzone w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t. j. Dz. U. 2023 poz. 913, z późn. zm.) – dalej „Ustawa”. W art. 89 Ustawy nałożono na ministra

właściwego do spraw informatyzacji zadanie polegające na utworzeniu i udostępnieniu systemu teleinformatycznego wymienionego w art. 46 ust. 1, wspierającego koordynację działań i współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, wypracowanie i przekazywanie rekomendacji podnoszących poziom cyberbezpieczeństwa, zapewnienie zgłaszania incydentów i umożliwiającego wspomaganie ich łagodzenia przez CSIRT GOV, CSIRT MON, CSIRT NASK oraz ostrzegania o zagrożeniach cyberbezpieczeństwa podmiotów KSC i zapewniającego obserwację ryzyka na poziomie krajowym.

W 2019 r. NASK PIB zostało zlecone zadanie publiczne polegające na „rozwoju systemu teleinformatycznego”, którego celem było dostosowanie produktów projektu NPC do wymagań Ustawy. W dniu 01.01.2021 r. system S46 został uruchomiony operacyjnie. W latach 2022 i 2023 NASK PIB realizował zadanie publiczne polegające na utrzymaniu i rozwoju systemu S46. W latach 2022-2023 NASK PIB realizował również zadanie „Podłączenie podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem S46 (S46-REACT)” mające na celu zwiększenie liczby podłączonych podmiotów, głównie JST i podmiotów z sektora ochrony zdrowia.

System S46 składa się z redundantnego systemu centralnego, wydzielonej sieci teleinformatycznej opartej na MPLS, podłączonych z jej wykorzystaniem uczestników (z zainstalowanymi u nich urządzeniami dostępowymi – SBU) oraz podłączonymi do systemu centralnego podmiotami KSC: CSIRT GOV, CSIRT MON, CSIRT NASK, organami właściwymi, Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa i innymi. W ramach prac finansowanych z budżetu państwa, planowane jest udostępnienie S46 poprzez Internet ww. podmiotom.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

| | |
|---|---|
| Cel - 1 | Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających dostęp do S46. |
| Cel strategiczny | 1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w szczególności cel 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej 2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności cel szczegółowy nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa. |
| Korzyść: | 1. osiągnięcie synergii poprzez włączenie do systemu dużej liczby podmiotów 2. Podniesienie skuteczności monitorowania ryzyk wiążących się z działaniem w cyberprzestrzeni RP znacznej liczby podmiotów. |
| KPI: | KPI1: Przedsiębiorstwa objęte wsparciem na opracowywanie lub przyjmowanie produktów, usług i procesów cyfrowych KPI2: Liczba podmiotów, którym udostępniono system dla co najmniej 385 podmiotów; |
| Wartość aktualna i docelowa KPI: | KPI1: Wartość aktualna: 0 KPI2: Wartość aktualna: 0 KPI1: Wartość docelowa: 60 KPI2: Wartość docelowa: 385 |
| Metoda | KPI1: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: |

| | |
|---|--|
| pomiaru KPI | <p>potwierdzenie udostępnienia systemu S46, zarejestrowane w systemach dokumentacyjnych NASK; częstotliwość pomiaru: rok po zakończeniu realizacji projektu;</p> <p>KPI2: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: potwierdzenie udostępnienia systemu S46, zarejestrowane w systemach dokumentacyjnych NASK; częstotliwość pomiaru: na koniec każdego kwartału kalendarzowego.</p> |
| Cel - 2 | Zwiększenie liczby pracowników posiadających umiejętność posługiwania się systemem S46, w podmiotach krajowego systemu cyberbezpieczeństwa. |
| Cel strategiczny | <p>1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w szczególności cel 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej</p> <p>2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności cel szczegółowy nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa.</p> |
| Korzyść: | <p>1. Poszerzenie wiedzy pracowników podłączanych jednostek w sferze zasad i sposobów wymiany informacji na temat cyberbezpieczeństwa przy pomocy S46.</p> <p>2. Zwiększenie świadomości sytuacyjnej podłączanego podmiotu oraz umożliwienie monitorowania ryzyk wiążących się z działaniem w cyberprzestrzeni.</p> |
| KPI: | <p>KPI3: Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych</p> <p>KPI4: Liczba użytkowników przeszkolonych z korzystania z systemu S46 (ogółem)</p> <p>KPI5: Liczba użytkowników przeszkolonych z korzystania z systemu S46 (kobiety)</p> <p>KPI6: Liczba użytkowników przeszkolonych z korzystania z systemu S46 (mężczyźni)</p> |
| Wartość aktualna i docelowa KPI: | <p>KPI3: Wartość aktualna: 0</p> <p>KPI4: Wartość aktualna (ogółem): 0</p> <p>KPI5: Wartość aktualna (kobiety): 0</p> <p>KPI6: Wartość aktualna (mężczyźni): 0</p> <p>KPI3: Wartość docelowa: 3000</p> <p>KPI4: Wartość docelowa (ogółem): 770</p> <p>KPI5: Wartość docelowa (kobiety): 77</p> <p>KPI6: Wartość docelowa (mężczyźni): 693</p> |
| Metoda pomiaru KPI | <p>KPI3: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: Liczba zakończonych powodzeniem prób uwierzytelnienia przy wykorzystaniu dostawcy usług (SP) w ciągu roku; częstotliwość pomiaru: na koniec realizacji projektu.</p> <p>KPI4: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: Lista osób przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK; częstotliwość pomiaru: na koniec każdego kwartału kalendarzowego.</p> <p>KPI5: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: Lista osób przeszkolonych z używania Systemu S46 zarejestrowanych w systemach dokumentacyjnych NASK; częstotliwość pomiaru: na koniec każdego kwartału kalendarzowego.</p> <p>KPI6: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: Lista osób przeszkolonych z używania Systemu S46 zarejestrowanych w</p> |

| | |
|---|--|
| | systemach dokumentacyjnych NASK; częstotliwość pomiaru: na koniec każdego kwartału kalendarzowego. |
| Cel - 3 | Zwiększenie wydajności systemu S46, zapewnienie obsługi zwiększonej liczby połączeń, udostępnienie usług samorejestracji podmiotów kluczowych i ważnych i dostosowanie mechanizmów komunikacji. |
| Cel strategiczny | 1/ Cele Programu Zintegrowanej Informatyzacji Państwa (PZIP) w szczególności cel 4.2.2. Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office) oraz 4.2.3. Podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów TIK oraz pracowników administracji publicznej 2/ Cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, w szczególności cel szczegółowy nr 1 – Rozwój krajowego systemu cyberbezpieczeństwa. |
| Korzyść: | System S46 zostanie doposażony, dzięki czemu zapewni: a) Zapewnienie bezpieczeństwa komunikacji przez Internet, dzięki przygotowaniu dedykowanego środowiska (strefa DMZ); b) Udostępnienie mechanizmu (samo)rejestracji podmiotów kluczowych i ważnych; c) Udostępnienie mechanizmów komunikacji dostosowanych do potrzeb podmiotów kluczowych i ważnych; d) redukcja kosztów korzystania z systemu S46 po stronie podmiotów kluczowych i ważnych; |
| KPI: | KPI7: Przedsiębiorstwa objęte wsparciem (w tym: małe, również mikro, średnie, duże) KPI8: Liczba uruchomionych usług samorejestracji podmiotów kluczowych i ważnych KPI9: Liczba uruchomionych usług wymiany informacji dostosowanych do potrzeb podmiotów kluczowych i ważnych; KPI10: Liczba zmodernizowanych systemów teleinformatycznych pod kątem wydajności i pojemności; |
| Wartość aktualna i docelowa KPI: | KPI7: Wartość aktualna: 0 KPI8: Wartość aktualna: 0 KPI9: Wartość aktualna: 0 KPI10: Wartość aktualna: 0 KPI7: Wartość docelowa: 1 KPI8: Wartość docelowa: 1 KPI9: Wartość docelowa: 1 KPI10: Wartość docelowa: 1 |
| Metoda pomiaru KPI | KPI7: Metoda pomiaru: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: protokół odbioru zmodernizowanego systemu S46; częstotliwość pomiaru: jednorazowo w dniu zakończenia projektu. KPI8: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: przyjęty pozytywnie raport z przeprowadzenia testów wydajnościowych i bezpieczeństwa obejmujący uruchomione usługi; częstotliwość pomiaru: jednorazowo w dniu zakończenia projektu; KPI9: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: przyjęty pozytywnie raport z przeprowadzenia testów wydajnościowych i bezpieczeństwa obejmujący uruchomione usługi; częstotliwość pomiaru: jednorazowo w dniu zakończenia projektu; KPI10: Metoda pomiaru: badanie ewaluacyjne ilościowe; źródło danych: |

przyjęty pozytywnie raport z przeprowadzenia testów wydajnościowych i bezpieczeństwa; częstotliwość pomiaru: jednorazowo w dniu zakończenia projektu.

2.2. Udostępnione e-usługi

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałości e-usługi |
|-----|---|------------|---|-----------------------------|
| 1 | Samorejestracja podmiotów kluczowych i ważnych – umożliwi podmiotom kluczowym i ważnym na obsługę cyklu życia wpisu w rejestrze. W szczególności umożliwi: rejestrację, weryfikację statusu wpisu do rejestru, wskazanie osób właściwych do spraw cyberbezpieczeństwa, czy aktualizację danych dotyczących podmiotu. Ze strony organów właściwych możliwe będzie obsługa wniosków o wpis, oraz wpisywanie podmiotów kluczowych lub podmiotów ważnych do wykazu z urzędu przez ministra właściwego do spraw informatyzacji i organy właściwe do spraw cyberbezpieczeństwa, czy wykreślenie z rejestru podmiotów KCS, jak również raportowanie. | A2A A2B | Podmioty kluczowe i ważne, podlegające procesowi samorejestracji na podstawie przepisów NIS2, z wyłączeniem Operatorów Usług Kluczowych Operatorzy Usług Kluczowych (nowelizacja ustawy o KSC wprowadzi pojęcie podmiotu kluczowego, które obejmie Operatorów Usług Kluczowych) Przedstawiciele podłączanych do S46 Operatorów Usług Kluczowych (zgodnie z aktualnie obowiązującą ustawą o KSC) Ministerstwo Cyfryzacji (rocznie ok 2000 transakcji) | Transakcja |
| 2 | Usługa wymiany wiadomości pomiędzy podmiotami kluczowymi i ważnymi oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa – dostosowana do potrzeb krajowego systemu bezpieczeństwa wymiana wiadomości będzie realizowana co najmniej w formie tekstowej z załącznikami, umożliwi podmiotom kluczowym i ważnym dwustronną komunikację indywidualną lub grupową (kierowaną do grup użytkowników zgodnie z klasyfikacją podmiotów KSC), w tym wymianę ostrzeżeń o podatnościach. | A2B A2A | Operatorzy Usług Kluczowych (nowelizacja ustawy o KSC wprowadzi pojęcie podmiotu kluczowego, które obejmie Operatorów Usług Kluczowych) Przedstawiciele podłączanych do S46 Operatorów Usług Kluczowych (zgodnie z aktualnie obowiązującą ustawą o KSC) Podmioty kluczowe i ważne, podlegające | Dwustronna interakcja |

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałości e-usługi |
|-----|----------------|-----|---|-----------------------------|
| | | | procesowi samorejestracji na podstawie przepisów NIS2, z wyłączeniem Operatorów Usług Kluczowych Ministerstwo Cyfryzacji (rocznie ok 2000 transakcji) | |

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

| Nazwa produktu | Planowana data wdrożenia |
|---|--------------------------|
| Zmodyfikowany system S46 w zakresie dodania usługi samorejestracji podmiotów kluczowych i ważnych, dostawcy usług (SP), wykazu podmiotów kluczowych i ważnych, dostosowania usługi wymiany wiadomości pomiędzy podmiotami kluczowymi i ważnymi i optymalizacji wydajności systemu s46 | 06-2026 |
| Podpisane umowy na elementy sprzętu i oprogramowania na potrzeby optymalizacji wydajności i pojemności systemu S46, w tym optymalizacji przetwarzania danych wykazu podmiotów kluczowych i ważnych | 04-2025 |
| Zakupione i zainstalowane urządzenia i oprogramowanie, na potrzeby optymalizacji wydajności i pojemności systemu S46, w tym optymalizacji przetwarzania danych wykazu podmiotów kluczowych i ważnych | 09-2025 |
| Makiety UX/UI dla wykazu podmiotów kluczowych i ważnych | 06-2024 |
| Raport z testów UAT platformy szkoleniowej | 03-2025 |
| Przygotowane materiały szkoleniowe | 10-2024 |
| Przygotowane materiały informacyjno-promocyjne | 10-2024 |
| Pozytywnie przyjęty raport z testów wydajności i bezpieczeństwa zmodernizowanego systemu S46 z dostosowaną usługą wymiany wiadomości | 06-2026 |
| Pozytywnie przyjęty raport z testów wydajności i bezpieczeństwa zmodernizowanego systemu S46 w zakresie wykazu podmiotów kluczowych i ważnych | 10-2024 |
| Uruchomiona platforma szkoleniowa | 03-2025 |
| Pozytywnie przyjęty raport z oceny efektywności szkoleń | 06-2026 |

3. KAMIENIE MIŁOWE

| Kamienie milowe | Planowany termin osiągnięcia |
|--|------------------------------|
| Uzyskany pozytywny wynik testów wydajnościowych i testów bezpieczeństwa wykazu podmiotów kluczowych i ważnych | 2024-10-15 |
| Uruchomiony wykaz podmiotów kluczowych i ważnych | 2024-10-30 |
| Przeprowadzone postępowania zakupowe na potrzeby optymalizacji wydajności i pojemności Systemu S46 i wykazu podmiotów kluczowych i ważnych | 2025-04-30 |
| S46 udostępniony dla minimum 150 podmiotów narastająco i przeszkolonych co najmniej 300 osób narastająco | 2025-06-30 |
| Dostarczone i zainstalowane urządzenia i oprogramowanie wymagane do zwiększenia pojemności Systemu S46 i podniesienia wydajności wykazu podmiotów kluczowych i ważnych | 2025-09-30 |
| S46 udostępniony dla minimum 225 podmiotów narastająco i przeszkolonych co najmniej 500 osób narastająco | 2026-02-01 |
| Uruchomiony zmodernizowany system S46 | 2026-06-30 |
| S46 udostępniony dla minimum 385 podmiotów narastająco i przeszkolonych co najmniej 770 osób narastająco | 2026-06-30 |
| Uzyskany pozytywny wynik testów wydajności i testów bezpieczeństwa zmodernizowanego systemu S46 z dostosowaną usługą wymiany wiadomości | 2026-06-30 |

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

| | | |
|---|---|---|
| Całkowity koszt projektu (netto oraz brutto), w tym | Netto 39 711 482,14 zł Brutto 41 741 692,14 zł | |
| Procent dofinansowania ze środków UE (brutto) | 95% | |
| Procent środków z budżetu państwa (brutto) | 5% | |
| Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto) | 2024 | Netto 11 532 517,86 zł Brutto 12 073 247,86 zł |
| | 2025 | Netto 20 085 476,19 zł Brutto 21 445 236,19 zł |
| | 2026 | Netto 8 093 488,09 zł Brutto 8 223 208,09 zł |

4.2. Wykaz poszczególnych pozycji kosztowych

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|---|---------------------------|--|
| Oprogramowanie | Koszty zakupu oprogramowania specjalistycznego, analiz, wytworzenia oprogramowania, testów, w tym testów funkcjonalnych integracyjnych, akceptacyjnych, przygotowania danych testowych, zasilenia inicjalnego, sanityzacji danych, korekt błędów, tworzenia prototypów. | 5 782 142,86 zł | Uruchomienie e-usług, wytwarzanie i modernizacja oprogramowania, obsługa zgłoszeń dotyczących błędów, korekty błędów, uruchomienie platform szkoleniowych. |
| Infrastruktura | Zakup urządzeń i wyposażenia, oprogramowania systemowego i wirtualizacyjnego, koszty wynagrodzeń personelu projektującego, wdrażającego i | 12 123 442,86 zł | Zapewnienie platformy niezbędnej do uruchomienia wykazu podmiotów kluczowych i ważnych, rozbudowa infrastruktury pod kątem wydajności. |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|---|
| | dokumentującego rozwiązania, korygującego błędy sprzętowe i systemowe i sieciowe, | | |
| Koszty UX i grafiki | Wynagrodzenia personelu i usługi obce dotyczące tworzenia makiet, współpracy z deweloperami i użytkownikami w zakresie realizacji projektu graficznego, wytwarzanie elementów graficznych i szaty graficznej, zbieranie opinii użytkowników dotyczących interfejsu UI. | 1 389 500,00 zł | Opracowanie warstwy wizualnej dla uruchamianych e-usług oraz materiałów dla użytkowników. |
| Bezpieczeństwo | Zakup urządzeń, usług obcych, wynagrodzenia personelu konfigurującego usługi i polityki bezpieczeństwa, realizującego testy bezpieczeństwa i tworzącego raporty bezpieczeństwa, koszty utwardzania systemu i realizacji rekomendacji wynikających z przeprowadzonych testów. | 9 015 866,86 zł | Zakup urządzeń (w tym pełniące funkcje HSM) i usług bezpieczeństwa (w tym oczyszczania ruchu), koszty personelu wdrażającego, projektującego, przygotowującego dokumentację wdrożeniową i operacyjną. |
| Wydajność rozwiązań | Wynagrodzenia w zakresie optymalizacji wydajności aplikacji, projektowania i realizacji testów wydajnościowych, tworzenia danych | 4 370 306,00 zł | Koszty wynagrodzeń personelu wdrażającego rozwiązania dedykowane poprawie wydajności, Koszty oprogramowania i infrastruktury ujęte osobno. |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|--|---|---------------------------|---|
| | testowych, tworzenia raportów z testów. | | |
| Szkolenia | Wynagrodzenia personelu szkolącego, organizującego szkolenia, tworzącego materiały szkoleniowe, w tym materiały e-learningowe, zarządzania i konfiguracji platformy szkoleniowej, raportowania wyników szkoleń. | 4 594 142,86 zł | Koszty szkoleń użytkowników, przygotowania materiałów, uruchomienia platformy e-learningowej |
| Działania informacyjno-promocyjne | Promocja i informacja (materiały i koszty inne) | 437 880,00 zł | Upowszechnianie wiedzy o konieczności i sposobach samorejestracji oraz podłączaniu do S46. |
| Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego) | Koszty pośrednie | 4 028 410,70 zł | Koszty wynajmu biura do celów realizacji projektu, mediów i materiałów koniecznych do działania biura (bez wyposażenia stanowisk pracy przeznaczonych w co najmniej 50% do realizacji obsługi rozbudowanego Systemu S46, ujętego w kosztach bezpośrednich), zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego, kierowników projektów, biura projektu, doradców prawnych) |

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

| | | | |
|--|------------------|---|---|
| Całkowity koszt utrzymania trwałości projektu (brutto) | 57 470 594,18 zł | | Źródło finansowania |
| Podział całkowitego kosztu utrzymania | 2026 | 4 728 867,00 zł (brutto) (3 919 630,00 zł netto) | krajowe środki publiczne - budżet państwa |

| | | | |
|---|------|---|---|
| trwałości projektu na poszczególne lata (netto oraz brutto) | 2027 | 8 042 301,30 zł (brutto) (6 678 716,00 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2028 | 8 846 531,43 zł (brutto) (7 346 587,60 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2029 | 9 731 184,57 zł (brutto) (8 081 246,36 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2030 | 20 234 343,03 zł (brutto) (16 637 371,00 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2031 | 5 887 366,85 zł (brutto) (4 889 154,20 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 |
|---|--------------------|--|---------------------------------------|--|
| Wzrost/zmiany kursu walut powodujący dezaktualizację szacunków cenowych dla urządzeń i oprogramowania | Średnia | | Średnie | - realizacja postępowań zakupowych odpowiednio wcześniej i z odpowiednim budżetem, tak aby dodatkowe ryzyko przenieść na Wykonawcę. - zawarcie w umowie z wykonawcą stosownych klauzul w zakresie zmian wpływających na wysokość wynagrodzenia za realizację przedmiotu zamówienia. |
| Niedostępność rozwiązań kompatybilnych z rozwiązaniami stosowanymi w S46, powodująca | Duża | | Średnie | - zmiany w harmonogramie projektu i dostosowanie go do materializujących się ryzyk. - poszukiwanie rozwiązań alternatywnych, które mogą być stosowane do zastąpienia |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|--|--------------------|---------------------------------------|---|
| konieczność zmiany zakresu projektu | | | niedostępnych rozwiązań. |
| Zmiany legislacyjne mogą wpłynąć na sposób bądź zakres realizacji zadania. | Duża | Średnie | - ścisła współpraca z ministrem właściwym do spraw informatyzacji, dostosowywanie zakresu do sygnalizowanych potrzeb |
| Nieosiągnięcie wszystkich planowanych korzyści | Duża | Niskie | - zwiększenie nakładów na promocję w przypadku braku osiągnięcia korzyści ze względu na braki informacyjne o usługach; - zwiększanie ilości przypisanych zasobów w celu przyspieszenia prac. |
| Utrata lub brak możliwości pozyskania personelu z kompetencjami niezbędnymi do realizacji projektu | Duża | Niskie | - monitorowanie zagrożeń związanych z utratą personelu; - zapewnianie zastępstw dla kluczowego personelu; - pozyskiwanie osób z odpowiednimi kompetencjami z rynku; - weryfikacja kompetencji podczas rekrutacji |
| Brak określonej części budżetowej, dla wydatków z budżetu państwa | Duża | Średnie | Negocjacje z Ministerstwem Finansów budżetu na sfinansowanie kosztów VAT i ustalenie części budżetowej, z której będzie realizowane finansowanie. |

5.2. Ryzyka wpływające na utrzymanie efektów

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|--|--------------------|---------------------------------------|---|
| Zmiany technologiczne powodujące konieczność przejścia na inne rozwiązanie | Duża | Średnie | - monitorowanie zmian na rynku; - wyszukiwanie alternatywnych rozwiązań; |
| Zmiany legislacyjne, modyfikujące | Duża | Średnie | - podejmowanie działań zaradczych na bieżąco - kontakt z legislatorami poprzez |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|---|--------------------|---------------------------------------|---|
| zadania systemu s46 | | | właściciela biznesowego systemu, w celu wprowadzenia poprawek redukujących ryzyko. |
| Utrata lub brak możliwości pozyskania personelu z kompetencjami niezbędnymi do utrzymania efektów realizacji projektu | Średnia | Niskie | <ul style="list-style-type: none"> - monitorowanie zagrożeń związanych z utratą personelu; - zapewnianie zastępstw dla kluczowego personelu; - pozyskiwanie osób z odpowiednimi kompetencjami z rynku; - weryfikacja kompetencji podczas rekrutacji |
| Brak wystarczających środków na utrzymanie efektów projektu | Duża | Niskie | <ul style="list-style-type: none"> - przegląd i planowanie z wyprzedzeniem budżetu na utrzymanie efektów realizacji projektu; - wprowadzenie niezbędnych środków do OSR nowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa |

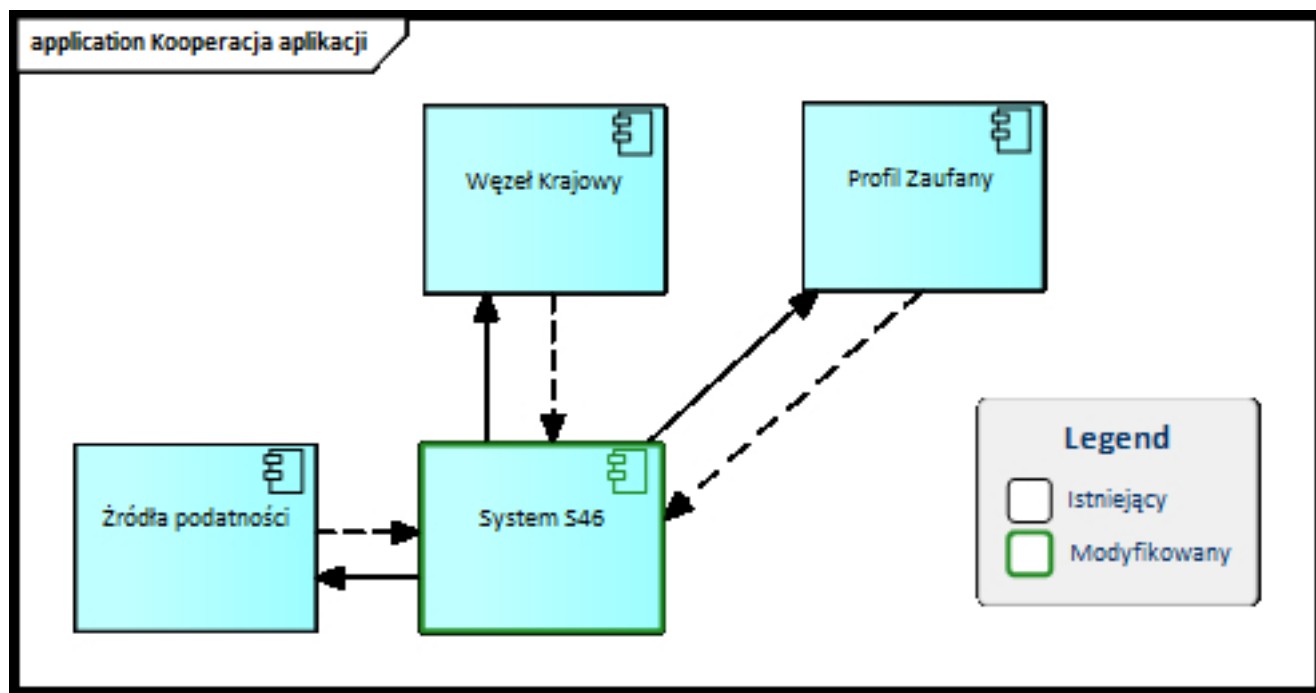
6. OTOCZENIE PRAWNE

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|--|------------------|--|--|
| 1 | Ustawa o Krajowym Systemie Cyberbezpieczeństwa (t. j. Dz. U. 2020 poz. 1369) | TAK/NIE | Umocowanie rejestru podmiotów KSC i usługi samorejestracji podmiotów KSC | Uzgodnienia międzyresortowe |
| 2 | Uchwała RM z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 | TAK/NIE | | |
| 3 | Ustawa z dnia 17 lutego 2005 o Informatyzacji działalności podmiotów realizujących zadania publiczne | TAK/NIE | | |
| 4 | Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów | TAK/NIE | | |

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|--|---------------------|----------------------------|--|
| | publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów informatycznych | | | |
| 5 | Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. | TAK /NIE | | |
| 6 | Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych | TAK /NIE | | |
| 7 | Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania | TAK /NIE | | |
| 8 | Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej | TAK /NIE | | |
| 9 | Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych | TAK /NIE | | |
| 10 | Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych | TAK /NIE | | |
| 11 | Uchwała Rady Ministrów w sprawie przyjęcia projektu Krajowego Planu Odbudowy i Zwiększania Odporności (IC9). Przyjęto: 30-04-2021 | TAK /NIE | | |

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w projekcie

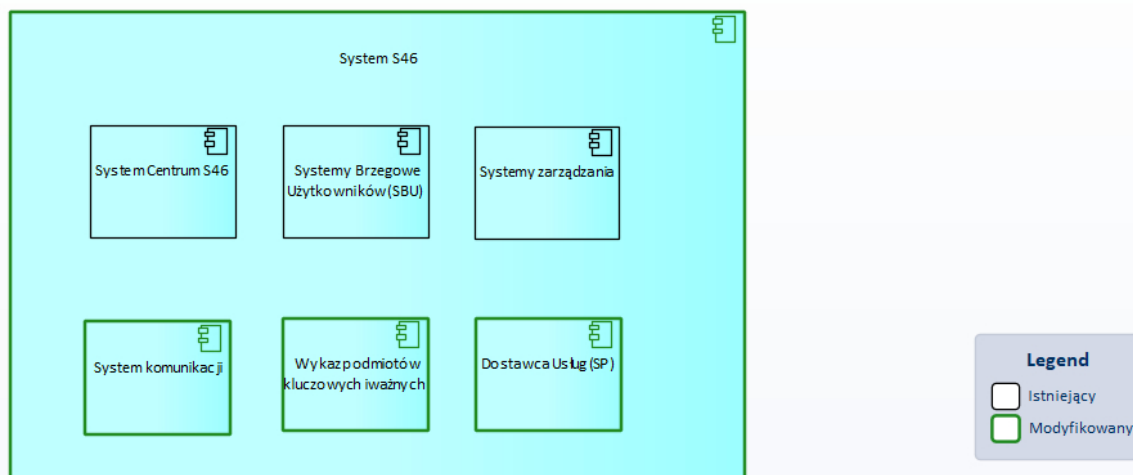
| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|---------------------|---|--------------|---|
| 1 | System S46 | Minister Cyfryzacji | System teleinformatyczny realizujący założenia systemu teleinformatycznego z art. 46 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa, S46 wspiera: współpracę podmiotów KSC, generowanie i przekazywanie rekomendacji, zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym, ostrzeganie o zagrożeniach cyberbezpieczeństwa. | Modyfikowany | Udostępnienie usługi samorejestracji podmiotu kluczowych i ważnych, wykazu podmiotów kluczowych i ważnych, dostawcy usług (SP), udostępnienie usługi wymiany informacji pomiędzy podmiotami ksc, dostosowanej do ich potrzeb; zwiększenie pojemności i optymalizacja wydajności |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|-------------------|-----------------------------------|---|------------|--------------------------------|
| | | | | | systemu. |
| 2 | Źródła podatności | Podmioty komercyjne , społeczność | Bazy danych podatności i zagrożeń, umożliwiające w zależności od rodzaju bazy: wyszukanie i pobranie informacji o podatnościach i zagrożeniach dotyczących konkretnych wersji produktów, informacji o zagrożonych sieciach komputerowych, botnetach, czy kampaniach phishingowych | Istniejący | |
| 3 | Węzeł Krajowy | Minister Cyfryzacji | Węzeł krajowy jest rozwiązaniem organizacyjno-technicznym umożliwiającym uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego | Istniejący | |
| 4 | Profil Zaufany | Minister Cyfryzacji | Profil zaufany jest środkiem identyfikacji elektronicznej. Dzięki niemu możliwe jest potwierdzenie tożsamości w Internecie oraz podpisanie dokumentu podpisem elektronicznym. | Istniejący | |

Lista przepływów

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-------------------|-------------------|--|----------------------------|--------------------------------|----------------------------|
| 1 | System S46 | Źródła podatności | Inicjowanie komunikacji; specyfikacja pobieranych podatności; | Tryb odwołań bezpośrednich | Krytyczny dla sukcesu projektu | Usługa REST API |
| 2 | Źródła podatności | System S46 | Informacje o podatnościach | Tryb odwołań bezpośrednich | Krytyczny dla sukcesu projektu | Format wymiany danych JSON |
| 3 | System S46 | Węzeł Krajowy | Inicjowanie komunikacji, żądanie identyfikacji (authentication request) | Tryb odwołań bezpośrednich | Krytyczny dla sukcesu projektu | Protokół SAML |
| 4 | Węzeł Krajowy | System S46 | Authentication Response, dane uwierzytelniane j osoby (asercja) | Tryb odwołań bezpośrednich | Krytyczny dla sukcesu projektu | Protokół SAML |
| 5 | System S46 | Profil Zaufany | Inicjowanie komunikacji, żądanie złożenia podpisu, skrót; dane do podpisania | Tryb odwołań bezpośrednich | Krytyczny dla sukcesu projektu | Protokół SOAP |
| 6 | Profil Zaufany | System S46 | Podpisany dokument, plik podpisu | Tryb odwołań bezpośrednich | Krytyczny dla sukcesu projektu | Protokół SOAP |

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

| Lp. | Obszar | Założenie technologiczne |
|-----|------------------------------|---|
| 1. | Infrastruktura | Stosowanie systemów zgodne z dotychczas używanymi (urządzenia HSM umożliwiające migrację materiału kryptograficznego, serwery umożliwiające dołączenie do istniejących klastrów, półki dyskowe zgodne z aktualnie wykorzystywanymi modelami urządzeń) |
| 2. | Sieć i bezpieczeństwo | Wykorzystanie zewnętrznego scrubbing center |
| 3. | Standardy wymiany danych | Stosowanie uznanych standardów komunikacyjnych takich jak SAML, WebService, SOAP, REST |
| 4. | Systemy operacyjne serwerowe | Stosowanie rozwiązań kompatybilnych z istniejącym rozwiązaniem |
| 5. | Bazy danych | Stosowanie rozwiązań kompatybilnych z istniejącym rozwiązaniem |
| 6. | Serwery aplikacji | Stosowanie rozwiązań kompatybilnych z istniejącym rozwiązaniem |
| 7. | Portale | Stosowanie rozwiązań kompatybilnych z istniejącym rozwiązaniem |
| 8. | Inne | |

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

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

| Lp. | Tworzony rejestr publiczny | Opis |
|-----|--------------------------------------|--|
| 1 | Wykaz podmiotów kluczowych i ważnych | <p>Zgodnie z propozycją nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa:</p> <p>„Art. 7.2. Wykaz, o którym mowa w ust. 1, zawiera:</p> <ol style="list-style-type: none"> 1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego; 2) sektor, podsektor i rodzaj podmiotu, zgodnie z załącznikiem nr 1 lub nr 2 do ustawy; 3) siedzibę i adres do korespondencji; 4) adres do doręczeń elektronicznych, jeżeli został nadany; 5) adres poczty elektronicznej; 6) numer identyfikacji podatkowej (NIP), jeżeli został nadany; 7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON); 8) numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany; 9) zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny; 10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny; 11) dane, co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej; 12) numer telefonu przyporządkowany do wykonywanej działalności; 13) deklarację podmiotu kluczowego lub podmiotu ważnego czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy; 14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność wraz z określeniem wykonywanej działalności; 15) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierające nazwę (firmę) dostawcy, siedzibę, adres, numer telefonu, adres poczty elektronicznej; 16) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5 ust. 4, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące: <ol style="list-style-type: none"> a) w przypadku osób fizycznych: imię i nazwisko, adres, numer telefonu oraz adres poczty elektronicznej, <p>[...]”</p> |

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